DOI 10.12694/scpe.v20i4.1586
Scalable Computing: Practice and Experience ISSN 1895-1767
Volume 20, Number 4, pp. 699–707. http://www.scpe.org © 2019 SCPE

APPLYING SEMANTIC WEB TECHNOLOGIES TO DISCOVER AN ONTOLOGY OF COMPUTER ATTACKS

ANDREI ZAMFIRA, RALUCA FAT, AND CĂLIN CENAN[*]

Abstract. The main scope of this paper is to present a methodology of engineering an ontology and to demonstrate how it is applied for designing and evaluating cyber-defense systems. The ontology is intended to be a vast model of the cybersecurity domain that captures a lot of information about attacks, source and target systems, methods, vulnerabilities exploited, consequences, controls for mitigation etc. For evaluating the quality of the proposed model we headed towards state-of-art methodologies comprised of a suite of metrics for assessing, among others: correctness, consistency, accuracy, completeness, soundness, task orientation. For the most important task, evaluation of efficacy in attacks detection, the proposed ontology was used as a knowledge model of a prototype web application firewall and we tested the system on a known evaluation dataset. The proposed system yielded a good detection rate and a low rate of false positives and negatives on the test data, and it was compared with other existing solutions in the field.

Key words: Ontology, data model, IDS, Semantic Web technology, knowledge representation and sharing

AMS subject classifications. 68Q55

1. Introduction.

Computer Security, also known in some places ”Cyber-Security” or ”IT security”, is the science that deals with the protection of computer systems from theft or damage to the hardware, software or data from them, as well from disruption or unauthorized use of their services. It includes controlling the physical access of hardware, protection against harm that come from network access, the malpractice by operators, either intentional or accidental. The field is of growing importance due to the reliance on Internet and computer networks of the society (e.g. Wi-Fi, Bluetooth etc), and the growth of ”smart devices”, such as mobile phones, television, devices from the Internet of Things etc [21].

Cybersecurity is critical in almost every industry that relies on computing equipment. Today most electronic devices (PCs, laptops, cellphones) come with built in firewalls software, but these do not make them 100% accurately protected against threats [2]. There are many ways in which computer systems can be hacked: using the network, download files from unsafe sites, connect to untrusted Wi-Fi networks, resource consumption, electromagnetic radiation etc. They can be protected through good software and hardware. By having strong internal interactions of properties, software complexity can prevent security failures and software crash [3]. The most important areas of industry that need protection against cybernetic threats are finances, aviation, automotive, industrial equipment, Internet of Things, among others.

Because this is what our current paper is intended to do, build a system that detects computer attacks, next we will present the reader with some basic notions and references where he can find more knowledge in the literature.

A system that is used in a suspicious situation to defend another system (or group) from the occurrence of cybernetic attacks is called an Intrusion Detection System (IDS). According to the NIST guide [6], the following is the definition of an IDS: ”intrusion detection is the process of monitoring the events occurring in a computer system or network and analyze them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable usage policies, or standard security practices. Intrusion prevention is the process of detection supplied with the capability to stop the possible incidents”.
Four types of IDSs are known today [4]:

- *network-based:* monitor network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify aware situations
- *host-based:* monitors the characteristics of a single host and the events occurring within it
- *wireless:* monitors wireless network traffic and analyze it to identify suspicious activity involving the wireless networking protocols
- *network behavior analysis:* examines network traffic to identify threats that generate unusual traffic flows, such as distributed denial of service (DDoS), certain forms of malware, and policy violations

[*] Politehnica University of Timişoara, Romania (andreizamfira@gmail.com)

The domain literature states that IDSs have gone through a few stages of evolution until present, that are:

- attacks signatures
- attack taxonomies
- attack ontologies

The first type of IDSs were signature-based, which means that they keep a syntactic representation of the attacks. This method is not very efficient due to many reasons, like attack signatures are not generic in nature, use specific languages related to particular domains and depend upon specific environments and systems, consequently they lack extensibility and dont suit for communication in heterogeneous environments. Attack signatures carry vague semantic information and lack solid ground of any formal logic, the smallest variation in business logic makes the signature invalid [5].

The second phase in the evolution of IDSs represented the use of taxonomies. Central components in the functionality of IDSs are taxonomies, which characterize and classify the attacks information, and a language to describe the instances of the taxonomy.

The current phase in IDSs evolution relies on the Semantic Web technologies, the principals are ontologies. Security systems built using an ontological approach are a promising new line of defense that can detect zero-day and sophisticated attacks because of the ability to capture the context of information and filter them by specific criteria [2]. Various generic security controls, like signature-based firewalls, intrusion detection and prevention systems or encryption devices have been developed, but their effectiveness against web-based threats is restricted due to their extreme rigidness. To obtain an efficient mitigation and stop the attack the system should understand the context of information to be processed and have the ability to filter the contents based on their effect on the target application. This is why security frameworks that rely ontologies are used in these situations [2].

An ontology is an explicit specification of the conceptualization of a domain which captures its context (interpretation of words in a specific domain). Ontological models are flexible in defining the concepts to desired level of detail, easily extensible and provide reasoning ability to reason over the instances of data of the domain. The fields of Artificial Intelligence and semantics use formal ontologies for knowledge sharing and reuse between software entities [3].

The main contributions of the current work are:

- ontological model of attacks: captures the context of important attacks, various of their technologies, sources and targets, consequences on the systems, vulnerabilities exploited and controls for mitigation of the attacks.
- a comprehensive best metrics suite for evaluation of the ontology in order to assess the quality of the proposed model; it includes: formal correctness, consistency, soundness, task orientation, completeness, conciseness, expandability, reusability and others.

2. Related Works. The use of semantic information in the development of security systems is an emerging research field that aims to create more effective defense systems that have a better performance in detecting the ever increasing in number and complexity of cybernetic attacks. The main part of technologies used in this area, such as ontologies, agents, neural networks, Bayesian filters, etc come mostly from the Semantic Web and Artificial Intelligence domains.

The current research represents a continuation of our work from [30]. This time, for the creation of our ontology we used a different development methodology, we took care to make a better description of each of its steps in order for the reader to better understand the process. For the evaluation phase, our ontology was tested for detection actual attacks using a commercial application firewall, Shadow Daemon, that has rules for detecting multiple types of attacks in computer networks, and we described the entire functionality of the system in order for the reader to understand how the process of detection is done, using figures and textual descriptions. This also hasn't been done in the other paper.

In [14] is presented a study made by a team from the MITRE corporation, as part of the JASON project, on the cybersecurity domain, to identify what is needed in creating a full-fledged science of Cybersecurity and recommend specific ways in which can be applied scientific methods. The study identified some fields of Computer Science that are most relevant and provided recommendations on further development of the science.

Razzaq [1] proposes two ontological models that store information from the cyber-security domain: one is about attacks that occur at the application level and the other captures information about HTTP communication protocol. He sustains that security frameworks built using ontological approaches are the next-gen line of defense because are able to capture the context of information.

Garcia-Teodoro et al. make in [11] a literature review of the techniques employed in building anomaly-based network NIDS systems, which he put into 3 categories: statistical-based, knowledge-based and machine-learning based. In the latter we find many techniques from the AI domain, such as Neural networks, Fuzzy logic, Markov models, Genetic algorithms, Clustering and outlier etc.

Papers [12] and [16] make a literary study about the use of an AI technology, namely Machine Learning in construction of detection systems. Compare the methods for intrusion detection based on the classifiers type: single, hybrid and ensemble.

In [6] also is sustained the idea of using ontologies in construction of intrusion detection systems. Propose an ontology to classify information about contexts of attacks that is used by a system to detect attacks at application level.

In [15] is presented an implementation of an IDS using Genetic Algorithms for detecting various types of intrusions in networks. This technology from AI uses evolution and natural selection that relies on a chromosome-like data structure and evolve the chromosomes using the operators of selection, recombination and mutation [18].

The most rightful guide in Computer Security and IDS systems is the recommendation of NIST (National Institute of Standards and Technology) in [6], which presents in large details (but not too broadly) what are the types of IDPS systems, capabilities and features of each one, how they are integrated and how is one selected for a special kind of activity.

In [17] is sustained the idea that a full-fledged science of cybersecurity has to be created in order to solve the problems related to vulnerabilities found in networks of computer systems. Its core principle is to cognize the cyberspace as a hybrid framework of interactions between humans and machines where security and privacy policies play a crucial role.

The contribution of our work compared to the ones presented above is that we do not only scratch the surface in building ontological models, but we tried to build a rigorous model by following state-of-art construction methodologies from the literature, and also to evaluate its capabilities by placing it in scenarios for which it was constructed to be used in the real applications. The experiments and results demonstrated that our ontological model behaves good for the scope for which it was created, that is improve the detection accuracy of IDS systems.

3. Building the Ontology. As it was stated in previous sections, an ontology is a specification in form of a data structure that captures the important concepts of an application domain and their relations. The process of ontology design is an iteration to determine its purpose, define concepts (classes), relations (properties), axioms, constraints and instances.

For the construction of our ontological model of cyber-attacks we chose the METHONTOLOGY development methodology. In [4] it is stated that this is the most mature methodology for ontologies engineering, as compared to others like Uschold and Kings, Gruniger and Foxs, or Bernaras methodologies.

In figure 3.1 can be seen the 6-steps process of constructing ontologies according to the METHONTOLOGY methodology [5].

Next we will try to explain this process from the perspective of developing our ontology.

Phase 1: Scope
The main scope of the proposed ontology in this paper is to express the complex knowledge of the cyber-security domain in a way that can be computationally traceable, machine processable and facilitate communication among software agents.

Phase 2: Elicitation
In order to obtain the necessary information to construct our knowledge model we studied various resources from the literature of cybersecurity, like catalogs, dictionaries and taxonomies of classes of attacks and malware, techniques used by hackers, target components, vulnerabilities exploited, consequences, etc. These sources include NISTs SCAP suite [28] (OVAL, CPE, CCE, CVE), CERT/CC Advisories, MAEC[26], CAPEC[27].

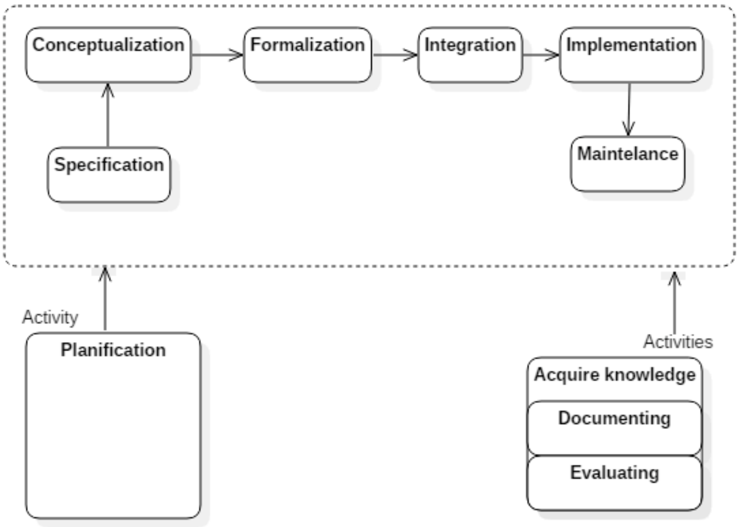

Fig. 3.1. *Phases of ontology development in METHONTOLOGY*

To acquire information about components of the ISO/OSI stack layers was studied the Internet Catalog of Assailable Technologies (ICAT), now called National Vulnerability Database (NVD) [31].

Phase 3: Conceptualization

After acquiring sufficient knowledge form the resources of cyber-security we were able to create our conceptual model by extracting the concepts (classes) and relations (properties) between them. The classes found are organized into a hierarchy of three levels, from the level of generalization they acquire. Classes from a lower level are sub-concepts of ones from superior levels.

In an ontology there are 3 types of properties: of objects, data and annotation. Object properties are relationships that links classes and objects. Data properties are attributes of classes that represents their structure. Annotation properties are sources of information that are attached to a class that says things about it. Facets of properties are restrictions that apply to properties, such as: data type, cardinality, quantifiers, hasValue restrictions.

Our ontological model comprises 106 classes, 38 object properties, 22 data properties and 3 annotation properties. In figures 3.2 and 3.3 are shown how classes and relations look in Protégé 4 editor.

Phase 4: Formalization

For the formal design of our conceptual model found so far we used a form of pseudo-code in which we expressed, in a top-down manner, our ontological system. We started with the complete model:

$$O = (C, P, A, I) \tag{3.1}$$

where C is the set of concepts, P the set of properties, A the set of axioms, and I the interpretation of the model. These can be further elaborated as:

$$C = (\cup_{t \in Type} C_t) \cup (\cup_{i \in Type} I_i) \tag{3.2}$$

$$P = (\cup_{p \in Type} P_p) \cup (\cup_{e \in Type} Rel_e) \tag{3.3}$$

$$A = (\cup_{a \in Type} A_a) \cup (\cup_{r \in Type} R_r) \tag{3.4}$$

where C is the set of all concepts with type t, I is the set of all instances with type i and P is the set of all properties with type p; Rel represents all relationships of type e , such as subsumption, equivalence and disjointness; A is a set of axioms and R a set of rules.

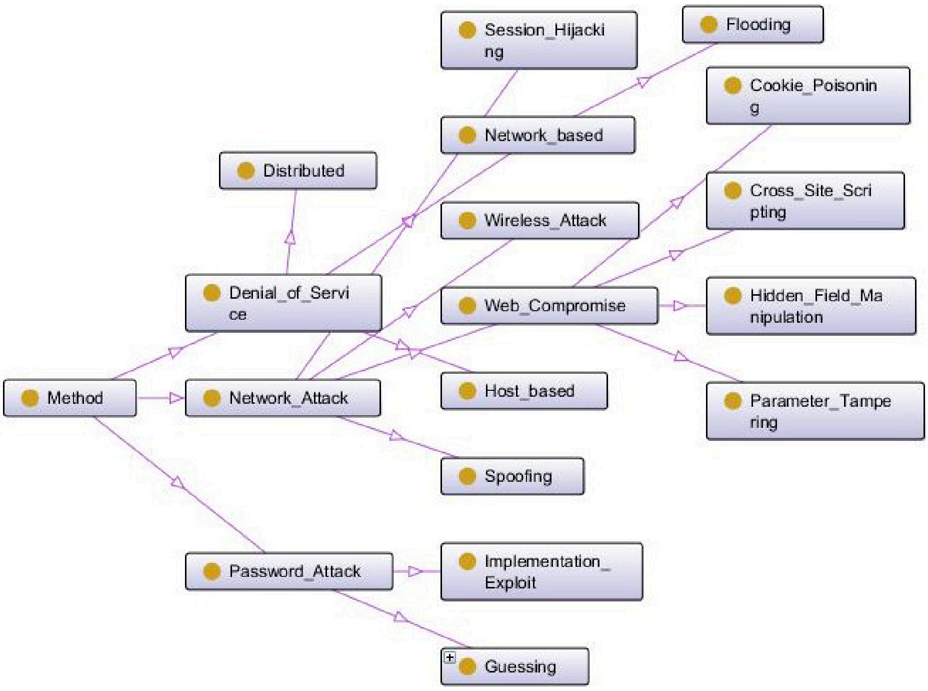

FIG. 3.2. *The owl:Method class and its subclasses*

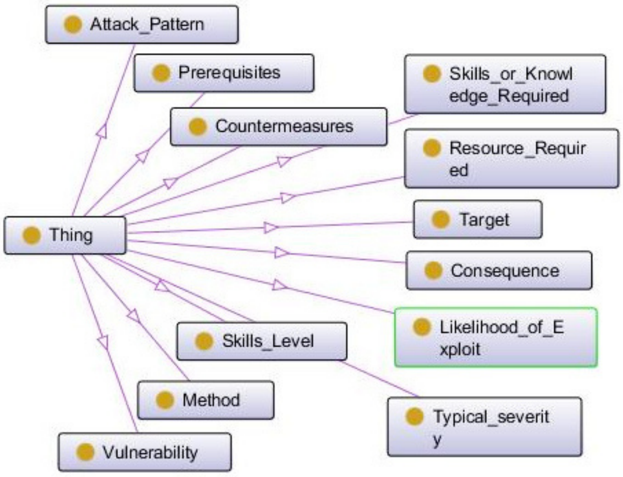

FIG. 3.3. *Top level classes of the ontology (OWLViz tool, Protege)*

Properties and relationships can be formally represented as:

$$P = (D : datatype, O : object, T : transitive, F : functional) \tag{3.5}$$

$$Rel = (\equiv : equivalence, \subseteq : subsumption, \cap : disjointnes) \tag{3.6}$$

Phase 5: Integration
This phase claims that ontologies must be created with the reuse goal in mind. To achieve this step for our ontology we chose a good formal language, OWL, and a development editor, so that when want to extend it to represent new knowledge we can easily do that by adding new axioms to the existing set.

Phase 6: Implementation
For the implementation we headed towards the state-of-art languages for ontologies construction, that is OWL second version, OWL 2.0. As the development editor we also chose currently best, that is Protégé 5 of Stanford University, California.

4. Evaluation. For the evaluation of our ontology we chose OntoClean [22], which we think it is the right methodology for our model. For other methodologies proposed in literature and a comparison of them reader is referred to [3].

Although in the literature there are stated more than 15 metrics for evaluation, we chose only 8 that we considered that are more relevant for our model, which will be discussed below.

Formal correctness: all information in the ontology must be accurate and valid according to existing standards of the domain modeled (in our case, cyber-security). OntoClean meta-properties rigid, identity and unity were applied to classes and properties of the ontology to ensure its correctness and checked for model specifications and subsumption relations violations using automated tools. Moreover, wrong patterns in the model had been detected and removed using SPARQL queries.

Consistency: according to [1] a model is consistent if all its relations are consistent and comply with its characteristics. We checked the consistency of our model by using the Pellet reasoner: the relations were verified in 66ms, class hierarchy in 264ms and inference was realized in 16ms.

Completeness: the proposed ontology by our work tries to be a large model that captures the domain as good as possible in order to increase the chances of the detection system to detect new and sophisticated attacks.

Expandability: it is possible to add new knowledge with minimum effort into our ontology using the process of semantic ontology alignment.

Clarity: each component of the ontology, i.e. concept, relation, axiom, rule is well stated and documented in order to be easily used, analyzed, understood etc.

Computational complexity, integrity, efficiency: the ontology was designed that does not generate and apply new rules each time a new situation occurs, to avoid redundant work of the system. Any change in the model may create new rules or regenerate existing instances. The semantic rules and constraints of the model are applied on concepts and properties, unlike signature-based techniques that have a less efficient way to capture contents of attacks and are prone to false positives.

Performance: the metrics for this criterion we chose from a bunch of many that were proposed in literature, as can be found in [30]: Detection rate (DR), Intrusion detection capability (CID), Area under ROC curve (AUC)[29].

Detection rate is defined as the ratio between number of correctly classified attacks and the total number of attacks.

$$CID = \frac{TP}{TP + FN} \tag{4.1}$$

CID is as an objective metric based on information theory that was proposed to solve the lacks and disadvantages of others existing. It takes into account all important aspects of detection capability, such as base rate B, positive predictive values (named also Bayesian detection rate - PPV), negative predictive values (NPV) and the probability of intrusions.

$$CID = -B(1-\beta)\log(PPV) - B(1-\beta)\log(1-NPV) - (1-B)(1-\alpha)\log(NPV) - (1-B)\alpha\log(1-PPV)$$

Receiver operating characteristics (ROC) curves are used on the one hand to visualize the relation between rates of detection and false positives of a classifier in its tuning phase, and also to compare the accuracy of several classifiers. Is computed with formula:

$$ROC = \frac{Sensitivity}{1 - Specificity} \tag{4.2}$$

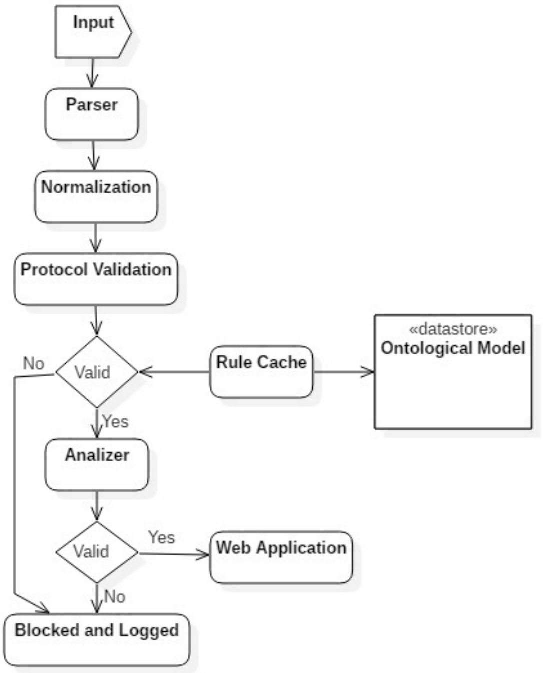

Fig. 5.1. *Ontology used by the detector*

where Sensitivity represents the fraction of true positives that are predicted as positives, and Specificity is the fraction of true negatives that are predicted as negatives. Area under the ROC curve is used as a summary of statistics [29].

Task orientation: this criterion ensures that the model fulfills the functional requirements for which it was developed. This will be proved during the course of the next section, where will be given details about the usage of the ontological model as part of the detection system.

5. Deployment. The proposed system is a novel approach for application of semantic technologies in the domain of information security. Various instances of attacks and vulnerabilities are tested using a prototype web application firewall. The ontology is stored into the firewalls knowledge base from where it is used by means of rules and inference to detect occurred situations. The use of semantic rules allows the system allows the model to be more time efficient because it provides substantial reduction in search space and yields low rates of false positives. The proposed system showed comparative detection rates to some of the best existing solutions today, like Snort and ModSecurity. In figure 5.1 is presented the architecture of the detection system, with its main modules.

Next we will try to explain how the process of detection is realized by the firewall. We will take as example a Cross Site Script (XSS) attack that a user injects into an application in an encoded form:

```
%3Cscript%3E%20alert(%22This%20is%20cross%20site%20)script%22)%20%3C%
2Fscript%3E%20site%20)script%22)%20%3C%2Fscript%3E
```

The input field is checked by the Parser for encoding, and in case yes then it is decoded; the above string decoded looks like:

```
<script>Alert("This is cross site scripting")</script>
```

After Normalization module, where it is transformed and rearranged by certain scales of the system, request is passed further to Protocol Validation and Analyzer modules.

In Protocol Validation and Analyzer the request is matched against the semantic rules that are generated

Table 6.1
Comparing our solution with existing systems

Metric Solution	Detection Rate	Detection Capability	Area under ROC
Ours	0.9050	0.8990	0.9071
Snort	0.9225	0.9031	0.9127
Suricata	0.8990	0.8750	0.8868
Bro	0.6780	0.5640	0.6688

by the ontological models from the KB for identification of malicious content in the input. Protocol Validation module is responsible for violations of protocol specifications, and the Analyzer for other attacks types. If the input content matches any of the generated rules then the request is blocked and is made a log with information about the attack found. Below is an example of a rule generated by the system from the ontological model.

```
[rule10: (?x rdf:type ex:HTTPRequest)  (?y rdf:typeex:ResponseHeaders)
         (?z rdf:type ex:ResponseSplitting)(?x ex:hasRequestHead) ?y)->(?x ex:hasAt ?z)]
```

6. Tests and Results. To test our ontology-based detection system on different types of attacks occurring in computer networks we used test datasets that are specifically created for this purpose. We chose KDDCup99 [23] since it is a medium size dataset that is more fit for our purpose. Other evaluation sets in this category are Kyoto2006+ [17], but this is too large and fit especially for IDSs of industrial scale.

Our system was compared to two state-of-art detectors existing today, Snort, Suricata and Bro [24]. Table 6.1 presents the results of evaluation of these systems based on three performance criterias stated in section 4.

The detection rate of the proposed system was very high, about 90%, very close to that of Snort and bigger than Suricata. The false alarm rate was 0.6%, also comparable to Snort.

7. Conclusions. In this work we proposed an ontology as a broad model of cyber-security domain, that tries to capture as much concepts and relations as possible in order to increase the performance of the detection system in which is used. It was constructed and evaluated using state-of-art methodologies in this purpose. For testing in detection of actual attacks in computer networks it was embedded into a web application firewall as its knowledge model, which consulted it each time to find out the nature of a new situation. The detection performance was compared to those of other 2 existing solutions today, and the results were comparable. The ontology can be downloaded from the authors drive account:

`https://drive.google.com/open?id=1NY7vBaoWQcI8QApP26SWaR8WY6bqJ1WK`

This paper represents only the beginning of our research in construction of Intrusion Detection and Prevention Systems (IDPS) to be used in various environments (hosts, LANs, wireless, etc). For now we limited only to an introduction into the domain and as contribution we created an ontological model using semantic technologies that can be used in detection activity. In the next chapter of our research we propose to move on and to actually implement an IDS that uses the proposed ontology in detecting the nature of situations from a host or network.

REFERENCES

[1] A.Razzaq, Z.Anwar, F.Ahmad, *Ontology for attack detection: An intelligent approach to web application security*, Computers & Security, Elsevier, vol.45 (2014).

[2] L.Obrst, P.Chase, R.Markeloff,*Developing an ontology for the cyber-security domain*, Semantic Technologies for Intelligence, Defense and Security (STIDS 2012)

[3] J.Hartman, P.Spyns, A.Giboin, D.Maynard, R.Cuel, *Methods for ontology evaluation*, EU-IST Network of Excellence (NoE), 2005

[4] F.Lopez, *Overview of methodologies for building ontologies*, International Joint Conference on Artificial Intelligence, 1999

[5] M.Fernandez, A.Gomez-Perez, N.Juristo, *METHONTOLOGY: From ontological art towards ontological engineering*, Association for the Advances in Artificial Intelligence, 1997

[6] K.Scarfone, P.Mell, *Guide to Intrusion Detection and Prevention Systems(IDPS)*, Reccomendations of the National Institute of Standards and Technology (NIST), Special Publication 2007

[7] F.Abdoli, M.Kahani, *Ontology-based Distributed Intrusion Detection System*, Proceedings of the 14th CSI Computer Conference (CSICC 09)

[8] N.Agarwal, S.Hussain, *A closer look at intrusion detection systems for web applications*, Hindawi Security and Communication Networks, 2018

[9] O.Can, M.Osman, E.Sezer, O.Bursa, B.Erdogdu, *An ontology-based approach for host intrusion detection systems*, 11th International Conference on Metadata and Semantic Research, Tallin, Estonia2017

[10] A.Razzaq, A.Hur, F.Ahmad, N.Haider, *Ontology-based application level intrusion detection system using Bayesian filter*, 2nd International Conference on Computer, Communication and Control, Budhapest, Hungary 2009

[11] P.Garcia-Teodoro, J.Diaz-Verdejo, G.Macia-Fernandez, E.Vazquez, *Anomaly-bases network intrusion detection: techniques, systems, challenges*, Elsevier, Computers & Security (2009)

[12] C.Tsai, Y.Hsu, C.Lin, W.Lin, *Intrusion detection by machine learning: A review*, Elsevier, Expert Systems with Applications, vol.36 (2009)

[13] M.Tavallaee, N.Stakhanova, A.Akbar,, *Towards credible evaluation of anomaly-based intrusion detection methods*, IEEE Transactions on Systems, Man and Cybernetics- Part C: Applications and reviews, vol.5 (2010)

[14] *Science of Cyber-security*, JASON Project, MITRE Corporation, McLean, Virginia (2010)

[15] M.Hoque, A.Mukit, A.N.Bikas, *An implementation of an intrusion detection system using a Genetic Algorithm*, International Journal of Network Security and Applications (IJNSA), vol.4 (2012)

[16] R.Sommer, V.Paxson, *Outside the closed world: On using machine learning for network intrusion detection*, IEEE Symposium on Security and Privacy (2010)

[17] P.McDaniel, B.Rivera, A.Swami, *Towards a Science of Secure Environments*, Journal of Security and Privacy, vol.12, pp.68-70 (2014)

[18] A.Oltramari, F.Cranor, J.Walls, *Building an ontology for cyber-security*, 9th International Conference on Semantic Technologies for Intelligence, Defense and Security, Fairfax, Virginia, USA (2014)

[19] S.Boubaker Ourida, *Implementation of an Intrusion Detection System*, International Journal of Computer Science, vol.9 (2012)

[20] Y.Lasheng, M.Chantal, *Agent-based distributed intrusion detection system*, Proceedings of Second International Symposium on Computer Science and Computational Technologies, Huangshang, China (2009)

[21] F.Vannel, N.Abdennadher, *Introduction to IoT*, https://docplayer.net/29316309-Introduction-to-iot-1.html

[22] N.Guarino, F.Welty, *Evaluating ontological decisions with OntoClean*, Communications on ACM, vol.45, pp.61-65

[23] P.Aggarwal, S.Sharma, *Analysis of KDD Dataset attributes - class wise for intrusion detection*, Procedia Compuer Science, vol.57, pp.842-851, Elsevier journal (2015)

[24] *2019 Open Source IDS tools - Snort, Suricata, Bro*, https://www.alienvault.com/blogs/security-essentials/open-source-intrusion-detection-tools-a-quick-overview, october 2018

[25] *MAEC: Malware Attribute Enumeration and Characterization*, https://maecproject.github.io/documentation/overview/

[26] *CAPEC: Common Attack Pattern Enumeration and Classification*, https://capec.mitre.org/

[27] *WASC Threat Classification*, http://projects.webappsec.org/w/page/13246978/Threat

[28] *SCAP: Security Content Automation Protocol*, https://www.open-scap.org/security-policies/scap-security-guide/

[29] M.Zweig, G.Campbell, *Receiver-operating Characteristics plots: A fundamental evaluation tool in clinical medicine*, Clinical Chemistry, vol.39, no.4, 1993

[30] A.Zamfira, H.Ciocarlie, *Developing an ontology for cyberoperations in computer networks*, Proceedings of 14th International Conference on Intelligent Computer Communication and Processing (ICCP'18)

[31] *NVD: National Vulnerabilities Database*, https://nvd.nist.gov/

Edited by: Dana Petcu
Received: Jul 28, 2019
Accepted: Oct 19, 2019