An Ontology Based Approach for Host Intrusion Detection Systems

Ozgu Can(✉), Murat Osman Unalir, Emine Sezer,
Okan Bursa, and Batuhan Erdogdu

Department of Computer Engineering, Ege University, 35100 Bornova-Izmir, Turkey
{ozgu.can,murat.osman.unalir,emine.sezer,okan.bursa}@ege.edu.tr,
batuhanerdogdu@gmail.com

Abstract. In recent years, cyber-attacks have emerged and these attacks result in serious consequences. In order to overcome these consequences, a fully-functioning and performance-improved intrusion detections systems are required. For this purpose, we used ontologies to provide semantic expressiveness and knowledge description for an intrusion detection system. In this work, a host intrusion detection system is implemented by using ontologies. The proposed system scans for malwares running on the operating system. Also, services and processes that are working on the system are scanned, and results are compared with the malware database. If any match occurs, the proposed system displays a malware list that matches with the information of that malware and where it is running. The proposed ontology based intrusion detection system aims to reduce the search time for malware scanning and to improve the performance of intrusion detection systems.

Keywords: Intrusion detection system · Host intrusion detection · Ontology · Semantic web

1 Introduction

Today, there are many types of computer security threats and these threats increase everyday. As a result of this increase, cyber-attacks have become a part of our daily lives. Cyber-attacks cause personal, financial, professional and also emotional damages. Unfortunately, most of the losses still can not be prevented. Thus, computer security has a significant importance in today's world and it is at the top of the international agendas. As there are several approaches to ensure security, Intrusion Detection System (IDS) is one of the critical detection approaches to protect computer systems. IDS, monitors the events in the computer or the network, analyzes them in order to detect the unauthorized or malicious activities within the computer or the network, and generates alerts when it observes potentially malicious activities. There are two types of IDS: Host IDS (HIDS) and Network IDS (NIDS). HIDS is an intrusion detection that monitors and analyzes the computer system, detects malicious activity and malwares on the host system, logs the activity and notifies the user. On the other hand, NIDS monitors and analyzes all the data passing through the network. The most effective protection is provided by a

E. Garoufallou et al. (Eds.): MTSR 2017, CCIS 755, pp. 80–86, 2017.
https://doi.org/10.1007/978-3-319-70863-8_8

combination of both NIDS and HIDS. Our proposed IDS model aims to provide both of these technologies in a single ontology-based IDS system.

In this work, an IDS ontology is developed and implemented by using Semantic Web technologies. As this is an ongoing work, the presented work is part of an HIDS. Therefore, the aim of the proposed system is to detect intrusions that may violate the security aspects of a computer system and to increase the performance of intrusion detection systems. For this purpose, we used ontologies as a database for the rule-based intrusion detection system. First, we created an IDS ontology. Later, all the processes and services that work on a computer system are added as individuals to the IDS ontology by using Facebook's osquery [1]. Also, we parsed malwares from Symantec's website [2] and added these malwares to the IDS ontology in order to compare with the processes and services that are working within the existing computer system. Finally, if any threat listed in the IDS ontology occurs in the working system, the proposed ontology based IDS system lists the malicious activities and malwares, and notifies the user. The paper is organized as follows: Sect. 2 presents the related work. Section 3 explains the IDS ontology. Section 4 presents the first implementation of the relevant ontology. Finally, Sect. 5 concludes and summarizes the future work.

2 Background

The purpose of our entire work is to implement a rule-based intrusion detection system by using Semantic Web technologies. Since IDS needs to monitor and analyze all the data passing through the network (NIDS) and processes in a single computer system (HIDS), the IDS needs to be very fast for this analysis in order to detect the malwares or malicious activities. Therefore, we used ontologies in order to use a semantic reasoner and a rule engine to detect intrusions and to improve performance of IDS. Also, the aim of the proposed model is to support both HIDS and NIDS for a better security. So far, as a result of our research, we have not found an ontology based IDS system that supports both HIDS and NIDS. And also, there is not much published research based on ontology use in IDS. In [3], an ontology is specified to model attacks. While the proposed attack ontology is based on DAML + OIL [4], our IDS ontology is based on OWL2 [5]. Also, our model and IDS ontology focus on IDS as a whole system, however the attack ontology just models attacks. An IDS based on ontology for web attacks is proposed in [6]. However, the proposed ontology and its concepts are inadequate to model an IDS system and just deals with web attacks. A rule status monitoring algorithm is given in [7]. The algorithm searches through the rules and reports whether they are enabled or disabled, and then reports it. This work does not use ontologies and Semantic Web technologies. In [8], a rule and a cluster based intrusion detection system for wireless sensor networks (WSN) is presented. The proposed system uses a relational database to store and manipulate data, and focuses on attacks in WSN. In our work, we focus on both HIDS and NIDS and use ontologies instead of relational database and osquery results instead of log-audit data.

3 IDS Ontology

An ontology is an explicit formal specifications of a conceptualization [9]. As a consequence, ontologies are used to share a common understanding among users or agents, to enable reuse of the domain knowledge, to analyze the domain knowledge, to make explicit domain assumptions and to separate the domain knowledge from the operational knowledge [10]. While developing the Intrusion Detection System (IDS) Ontology, we used the ontology development steps defined in [10].

The IDS ontology has been developed to implement an intrusion detection system that examines the processes and services of a device and the devices connected to the network, and also the packets on the network to which these devices are connected. As this is an ongoing work, IDS ontology is still being developed.

In the IDS ontology, the enumerated IDS terms are listed as: `Device`, `DatabaseServer`, `ManagedDevice`, `NetworkManagementSystem`, `Packet`, `SignaturedPacket`, `Process`, `Service`, `Software`, `Malware`, `destination`, `destinationMac`, `destinationPort`, `information`, `ack`, `fin`, `payload`, `syn`, `win`, `name`, `os`, `protocol`, `source`, `sourcePort`, `sourceMac`, `type`. The classes, object and data type properties defined in the IDS ontology are shown in Figs. 1, 2 and 3, respectively.

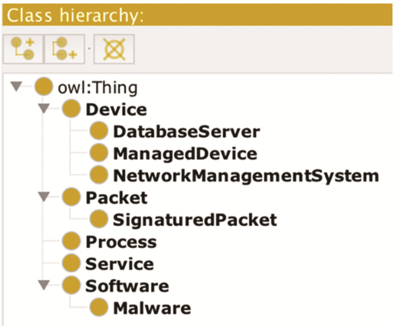
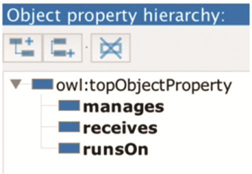


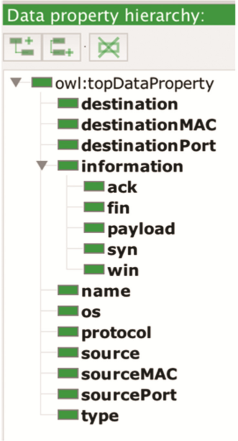
Fig. 1. The class hierarchy of IDS ontology.



Object property hierarchy:

owl:topObjectProperty
- manages
- receives
- runsOn

Fig. 2. The object property hierarchy of IDS ontology.



Data property hierarchy:

owl:topDataProperty
- destination
- destinationMAC
- destinationPort
- information
  - ack
  - fin
  - payload
  - syn
  - win
- name
- os
- protocol
- source
- sourceMAC
- sourcePort
- type

Fig. 3. The data property hierarchy of IDS ontology.

The classes are defined according to the following purposes: Device is used to store the devices in the network, DatabaseServer is used to store the list of malwares and harmful packets. The list will be taken from Symantec's [2] website, ManagedDevice is used to store devices that are controlled in the network, NetworkManagementSystem is used to store devices that in which the intrusion detection system is executed, Packet is used to store the packets that come from internet, SignaturedPacket is a subclass of Packet and used to store harmful or malicious packets, Process is used to store processes that work in the device, Service is used to store services that work in the device, Software is used to store software, Malware is a subclass of Software and used to store malwares that are detected in the device.

The object properties are defined according to the following purposes: manages is the action of a NetworkManagementSystem (Network Management System) to manage other ManagedDevices on the network, receives is the action of receiving a Packet from a Device, runsOn is the action of the Software in a Device. Table 1 shows the domain and range information for the defined object properties.

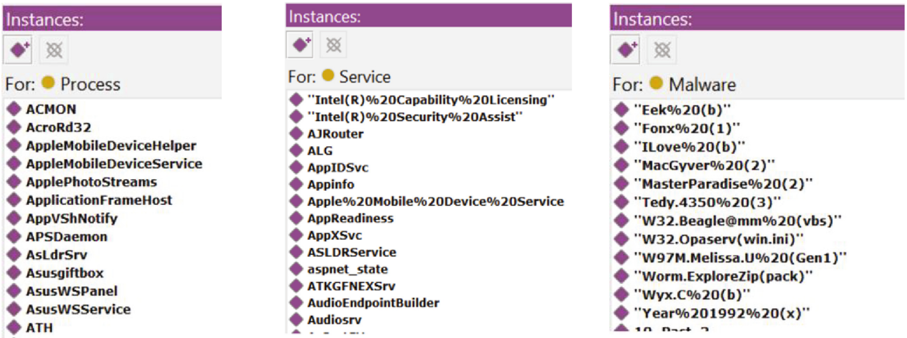
Table 1. Domain and Range information of the object properties.

Name	Range	Domain
manages	ManagedDevice	NetworkManagementSystem
receives	Packet	Device
runsOn	Device	Software

The data properties are defined according to the following purposes: destination is the final device that the Packet arrives, destinationMAC is the MAC address of the Packet's destination, destinationPort is the port number of the Packet's destination, information is the data in the Packet, ack is the signal to acknowledge the receipt of the Packet, fin is used to give information about whether the Packet transfer is finished or not, payload is the essential data that is being carried within a Packet, syn is used for synchronization with the Packet source, win is used for the window size, os is the operating system of the Device, source indicates the Device where the Packet comes from, sourceMAC is the MAC address of the Packet's source, sourcePort is the port number of the Packet's source, type is the type of the malware (for example: Virus, Trojan, etc.).

4 Implementation

In order to detect intrusions by using IDS ontology, first we parsed malwares from Symantec's website [2] to a csv file. Then, by using Jena [11], these malwares are written as individuals to IDS ontology's Malware class. We used Facebook's osquery [1] to create the individuals of Process and Service classes. These individuals belong to the working computer system. The automatically added individuals of Process and Service classes, and Malware classes are given in Fig. 4.



ACMON
AcroRd32
AppleMobileDeviceHelper
AppleMobileDeviceService
ApplePhotoStreams
ApplicationFrameHost
AppVShNotify
APSDaemon
AsLdrSrv
Asusgiftbox
AsusWSPanel
AsusWSService
ATH

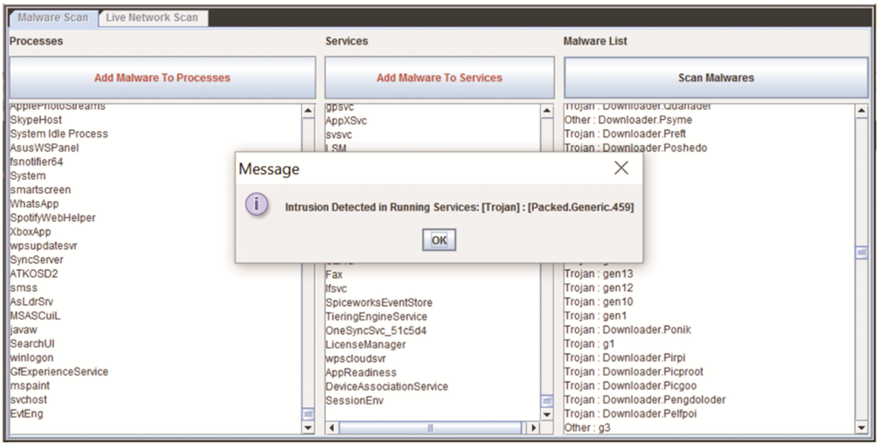
"Intel(R)%20Capability%20Licensing"
"Intel(R)%20Security%20Assist"
AJRouter
ALG
AppIDSvc
Appinfo
Apple%20Mobile%20Device%20Service
AppReadiness
AppXSvc
ASLDRService
aspnet_state
ATKGFNEXSrv
AudioEndpointBuilder
Audiosrv

"Eek%20(b)"
"Fonx%20(1)"
"ILove%20(b)"
"MacGyver%20(2)"
"MasterParadise%20(2)"
"Tedy.4350%20(3)"
"W32.Beagle@mm%20(vbs)"
"W32.Opaserv(win.ini)"
"W97M.Melissa.U%20(Gen1)"
"Worm.ExploreZip(pack)"
"Wyx.C%20(b)"
"Year%201992%20(x)"

(a) Process (b) Service (c) Malware

Fig. 4. Individuals of Process, Service and Malware classes.

The implementation compares the individuals of Malware class with the individuals of Process and Service classes to detect intrusions. If it finds a match between individuals in these classes of the IDS ontology, then an intrusion is detected and a warning message is shown as seen in Fig. 5.



Intrusion Detected in Running Services: [Trojan] : [Packed.Generic.459]

ApplePhotoStreams
SkypeHost
System Idle Process
AsusWSPanel
fsnotifier64
System
smartscreen
WhatsApp
SpotifyWebHelper
XboxApp
wpsupdatesvr
SyncServer
ATKOSD2
smss
AsLdrSrv
MSASCuiL
javaw
SearchUI
winlogon
GfExperienceService
mspaint
svchost
EvtEng

gpsvc
AppXSvc
svsvc
LSM
Fax
lfsvc
SpiceworksEventStore
TieringEngineService
OneSyncSvc_51c5d4
LicenseManager
wpscloudsvr
AppReadiness
DeviceAssociationService
SessionEnv

Trojan : Downloader.Quanader
Other : Downloader.Psyme
Trojan : Downloader.Preft
Trojan : Downloader.Poshedo
Trojan : gen13
Trojan : gen12
Trojan : gen10
Trojan : gen1
Trojan : Downloader.Ponik
Trojan : g1
Trojan : Downloader.Pirpi
Trojan : Downloader.Picproot
Trojan : Downloader.Picgoo
Trojan : Downloader.Pengdoloder
Trojan : Downloader.Pelfpoi
Other : g3

Fig. 5. Detecting intrusion in a computer system.

5 Conclusion

As information technology has become a key component for critical infrastructures, intrusion detection systems also become increasingly important due to the increased cyber-attacks in recent years. Our project aims to develop an ontology based IDS including both NIDS and HIDS for an effective security. As this is an ongoing project, in this work, we developed an IDS ontology and implemented this ontology to detect intrusions in a computer system. The proposed work is a part of HIDS. As a future work, IDS ontology will be extended according to provide NIDS. For this purpose, Live Network Scan tab seen in Fig. 5 will be activated and pcap4j [12] library will be used for the implementation. Besides, log analysis, event correlation and policy enforcement will be added to the intended ontology-based IDS model. New rules will be added in order to detect which devices are affected by interprocess dependencies and which processes are affected from which malwares.

References

1. Facebook Osquery, SQL powered operating system instrumentation, monitoring, and analytics. https://github.com/facebook/osquery. Accessed 08 July 2017
2. Symantec: Security Response. https://www.symantec.com/security_response/landing/azlisting.jsp. Accessed 08 July 2017
3. Undercoffer, J., Joshi, A., Pinkston, J.: Modeling computer attacks: an ontology for intrusion detection. In: Vigna, G., Kruegel, C., Jonsson, E. (eds.) RAID 2003. LNCS, vol. 2820, pp. 113–135. Springer, Heidelberg (2003). doi:10.1007/978-3-540-45248-5_7
4. DAML + OIL Reference Description Homepage. https://www.w3.org/TR/daml+oil-reference. Accessed 08 July 2017
5. OWL2 Homepage. https://www.w3.org/TR/owl2-overview/. Accessed 08 July 2017

6. Khairkar, A.D.: Intrusion Detection System based on Ontology for Web Applications. Dissertation, Master of Technology, Computer Engineering, Department of Computer Engineering and Information Technology College of Engineering, Pune (2013)
7. Turner, C., Rolston, J., Richards, D., Joseph, A.: A rule status monitoring algorithm for rule-based intrusion detection and prevention systems. Procedia Comput. Sci. **95**, 361–368 (2016)
8. Deshmukh, R., Deshmukh, R., Manoj Sharma, M.: Rule-based and cluster-based intrusion detection technique for wireless sensor network. Int. J. Comput. Sci. Mobile Comput. **2**(6), 200–208 (2013)
9. Gruber, T.R.: A translation approach to portable ontologies. Knowl. Acquisition **5**(2), 199–220 (1993)
10. Noy, N.F., McGuinness, D.L.: Ontology Development 101: A Guide to Creating Your First Ontology. http://protege.stanford.edu/publications/ontology_development/ontology101.pdf. Accessed 08 July 2017
11. Apache Jena Homepage. https://jena.apache.org. Accessed 08 July 2017
12. Kaitoy Pcap4J: A Java library for capturing, crafting, and sending packets. https://github.com/kaitoy/pcap4j. Accessed 08 July 2017