Ontological IDS Monitoring on Defined Attack

Vinod Kumar Shukla[1], D. B. Ojha[2]

[1]Research Scholar, Mewar University, Chittorgarh, Rajasthan, India

[2]Professor, Mewar University, Chittorgarh, Rajasthan, India

Abstract: ***Internet growth has become the challenge for the internet security. Our paper is divided into four sections. Section –I is introduction. Section – II is based on the concepts of SNMP, MIB, IDS and Ontology. In subsequent sections there is discussion about our proposed method in which, we have taken a model of manager and agent communication. All agents in one network communicate to one manager. Manager take the responsibility for identifying and defining the new type of Intrusion based on communication done between manager and agent. If intrusion is confirmed then immediately and ontology will be formed by manager and communicated to all managed devices in network with the help of Ontology, it will help all the managed devices on the network to update their intrusion signature database. By this all the devices on the network can be more secure and monitoring will be more updated.***

Keywords: SNMP, MIB, IDS, Onotology, OWL-DL

1. Introduction

With the immense growth of Internet users, Security on internet also became a challenge to implement. With the increase in the size and number of computer networks, the need for efficient management of network resources has emerged as alarming issue for network security. Network management is vital for optimized, controlled, and cost efficient utilization of network resources [1]. We can refer network security as group of policies and procedures implemented to avoid and keep track of unauthorized access, exploitation, modification, or denial of the network and network resources. Network security is required to all type of resources which operates on computer network. There are various tools and methods are available for network security. By implementing the IDS (Intrusion Detection System) concept, network security and network monitoring can be done more precisely.

Our proposed system works on the concept of Master Agent and Host agent. Master agent works on the server, and Host agent on the connect clients with servers. Master agent communicates with all the clients with the help of SNMP protocol. If there is some activity which is not defined in signature databases then this immediately need to be informed to each device on that network i.e. server and to client both need to update their signature database with new type of Intrusion definition. As soon as the detection is confirmed, immediately after that, ontology will be formed from server and will be sent to the entire associated Managed object. Ontology will be formed on the some basic characteristics, after the NIDS will confirm and define this new attack into its signature database.

Figure 1: Communication model of Manager and Agent

Our suggested methodology for Intrusion detection system is based on

Section – II

The following paper is based on the discussion of *SNMP, MIB, IDS and Ontology (OWL-DL language).*

2. SNMP

Simple Network Management Protocol (SNMP) is a popular protocol for network management. It is used for collecting information from, and configuring, network devices, such as servers, printers, hubs, switches, and routers on an Internet Protocol (IP) network. [2] Since its creation, Simple Network Management Protocol (SNMP) has been the solution for managing network elements in ever-growing various network types and has achieved widespread acceptance because of its simplicity [3].

SNMP has become the standard for the exchange of network information. SNMP managed network devices work on concept of manager/agent that executes all the MIB objects that are relevant. The agent provides the information contained in the MIB to management applications when it is needed. SNMP polls for information gathered by a network agent. The agent collects data from the network device it is located on and stores it in the MIB. When polled, the agent will send the information back to the SNMP manager. A manager or management system is a separate entity that is responsible to communicate with the SNMP agent implemented on network devices. Main function of SNMP Manager are to queries with agents, gets responses from agents, sets variables in agents and acknowledges asynchronous events from agents and the main functions of SNMP agent are to collect management information about its local environment, stores and retrieves management information as defined in the MIB, signals an event to the manager, acts as a proxy for some non–SNMP manageable network node.

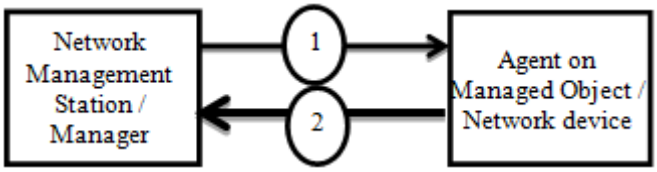


Figure 2: Set and Get request between Manager and Agent

1. The Manager sends request to managed objects.
2. The Agent responds to Manager for the request made by Manager.

SNMP is a popular protocol for uses and for the implementation point of view as well because it has a set of commands which are very concise are listed below. [4]

Table I: SNMP Commands

SNMP Commands	*Description*
GET	The GET operation is a request sent by the manager to the managed device. It is performed to retrieve one or more values from the managed device.
GET NEXT	Similar to the GET. GET NEXT operation retrieves the value of the next OID in the MIB tree.
GET BULK	The GETBULK operation is used to retrieve voluminous data from large MIB table.
SET	This operation is used by the managers to modify or assign the value of the Managed device.
TRAPS	TRAPS are initiated by the Agents. It is a signal to the SNMP Manager by the Agent on the occurrence of an event.
INFORM	INFORM includes confirmation from the SNMP manager on receiving the message.
RESPONSE	It is the command used to carry back the value(s) or signal of actions directed by the SNMP Manager.

These commands help SNMP manager and SNMP clients for information exchange. Every SNMP agent maintains an information database describing the managed device parameters. The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the Network Management System (NMS). This commonly shared database between the Agent and the Manager is called Management Information Base (MIB).

The basic communication architecture of SNMP is straightforward; there are three types of requests and one unsolicited information transmission.

To get information from an SNMP device, a "manager" will send a "GetRequest" or "Get"NextRequest" to an "agent" and the requested information or an error message will be sent back in a "Response." If a manager wants to modify information on an agent, a "SetRequest" will be sent with a corresponding response to confirm or report an error.

The unsolicited message form is called a "trap." This kind of message is usually sent by agents on start-up, on status change and in response to error conditions. [5]

3. MIB (Management Information Base)

Network devices which are managed by SNMP they need to implement the MIB (Management Information Base), the management application must be configured for what can be managed on the agent. A management information base (MIB) is a formal description of a set of network objects that can be managed using the Simple Network Management Protocol (SNMP). MIB module files are loaded into the NMS (Network Management System) so that the device can be managed. [6]

The **management information base** (**MIB**)**is** the repository of all management information being used in a Network Management Platform. In fact, MIB is a conceptual framework that encapsulates a certain "view" of the network entities being useful for the management purpose and the relationship between these entities [7]. These entities are called **Managed Objects**. A managed object is an abstraction of network resources such as host, modem, protocols and application entities. The task of Network Management is accomplished by the communication between manager and agent by means of a protocol to manipulate this managed object. [8]

A **management information base** (**MIB**) is a virtual database used for managing the entities in a communications network. The information on the agent is stored in what is called a Management Information Base (MIB). This is a hierarchical data structure that describes all the "objects" that a device can report the status of and, in some cases, set the value of.

The MIB contains the name, object identifier (a numeric value), data type and indication of whether the value associated with the object can be read from and/or written to.A manageable device is known an agent and a computer that is used to work with an agent is called a network management station (NMS). The management software that runs on an NMS is called a management application.

4. Intrusion

As the use of computer system increases; intrusions against them increase too. Intrusion is a set of actions which attempt to compromise the confidentiality, integrity or availability of a resource [9]. Intrusion detection system plays an important role in Network security. An intrusion detection system (IDS) inspects all inbound and outbound network activity and identifies suspicious patterns that may indicate a network or system attack from someone attempting to break into or compromise a system [10]. IDS systems are very popular and the main reason for this is they are very easy to deploy (as there is no need to change the existing infrastructure), less cost (as these systems can be installed for all the network segments, so it eliminates the requirement of software at each host in a network segment), and detect attacks and many other.

Intrusion detection is the process of identifying potential threats to networks, computers, databases and other IT devices. Intrusion detection has become increasingly essential with the growth of the Internet. It has become the need for the organization to implement this to prevent themselves from hackers. Intrusion detection works by collecting information and then examining it for inappropriate occurrences. Network administrator uses this data to take future preventative measures and make improvements to network security.

IDS keep track of all kind of communication from a particular place its main objective is to detect attacks and provide real time monitoring, if detected then to provide the solution for that and to record the attack definition. It analyzes the traffic on network to monitor signs of different malicious activity. In reality, an intrusion detection system does not detect the intrusion itself, but rather identifies the evidence to suggest that an intrusion is in progress or has already occurred. Following are some very common properties of IDS.

Table 2: Common properties of IDS

Traffic Collector	In HIDS this component analyses the data for inbound and outbound traffic analysis. In NIDS this will pull data off a segment of a network for analysis.
Analysis Engine	All the data collected by traffic collector analyzed by analysis engine. It is analyzed with comparison to signature database to see the pattern of behavior and other related activity.
Signature Database	Signature database contains a collection of signatures known to be associated with suspicious and malicious activities.
Management & Reporting Interface	A management interface providing a mechanism by which system administrators can manage the system and receive alerts when intrusions are detected.

An intrusion detection system can be run manually but most IT administrators find it easier to automate the system checks to ensure that nothing is accidentally overlooked. It is also necessary to cover all of the bases when it comes to a system check so that statistical analysis can be performed accurately. [11]

Intrusion detection systems are typically grouped into one of two categories:

Host-based IDS - A *Host-Based IDS* monitors the activity on individual systems with a view to identifying unauthorized or suspicious activity taking place on the operating system. Different type of properties are monitored by some central server, which are installed in HIDS, some of them are in following Table.

Table 3: Properties of HIDS

HIDS Property	*Description*
Log Analyzer	Concern for the unauthorized access on internal system, if any entry in log matches some criteria on Host based system them immediate action will be taken.
Signature Based Sensor	Good for tracking the unauthorized access and matches the traffic with its defined signature policy, if deviated then issues the warring to the Host based IDS system.
System call analyzer	Analysis the calls between the applications and operating system to identify the security event, when application want to start the event this goes for check to the operating system to match with defined signature.
Application behavior analyzer	It examines the call initiated by the application, that application is allowed to start the call or this is initiated to check that it looks like the attack.
File integrity checker	Checks for the integrity in file with the help of cryptographic check and digital signature of the file, periodically each monitored has its signature recomputed and compared to original.

Network-based IDS- Network-Based IDS is solely concerned with the activity taking place on a network (or more specifically, the segment of a network on which it is operating) [12]. Network-based intrusion detection systems (NIDS) monitor traffic passing through a network and compare that traffic with its signature database known to be associated with malicious activity. A number of different signature properties are used by the typical NIDS:

Table 4: Properties of NIDS

NIDS Property	*Description*
Header Signatures	Scans the header portion of network packets to identify suspicious or inappropriate information.
Port Signatures	Monitors the destination port of network packets to identify packets destined for ports not serviced by the servers on the network, or targeting ports known to be used by common attacks.
String signatures	Identifies strings contained in the payload of network packets to identify strings known to be present in malicious code.

5. Ontology

Ontology refers to the interpretation of a group of ideas within a specific domain that defines the interrelationship between those ideas. Ontology can be used to study the existence of entities within a specific domain and sometimes can be used to identify the domain itself [13].

Ontologies can enhance the functioning of the Web in many ways. They can be used in a simple fashion to improve the accuracy of Web searches—the search program can look for only those pages that refer to a precise concept instead of all the ones using ambiguous keywords. More advanced applications will use ontologies to relate the information on a page to the associated knowledge structures and inference rules. [14] The advantage of ontology is that it represents real world information in a manner that is machine process able. The reason ontologies are becoming popular is largely due to what they promise: a shared and common understanding of a domain that can be communicated between people and application systems. Specifically, ontologies offer the following benefits: [15]

- They assist in the communication between humans. Here, an unambiguous but informal ontology may be sufficient.
- ***They achieve interoperability among computer systems achieved by translating between different modeling methods, paradigms, languages and software tools. Here, the ontology is used as an interchange format.***
- They improve the process and/or quality of engineering software systems.

With respect to computer-based modeling, ontologies have the following advantages: [15]

- **Re-Usability:** the ontology is the basis for a formal encoding of the important entities, attributes, processes and their inter-relationships in the domain of interest. This formal representation may be a reusable and/or shared component in a software system.
- **Search:** Ontology may be used as metadata, serving as an index into a repository of information.
- **Knowledge Acquisition:** using an existing ontology as the starting point and basis for guiding knowledge

acquisition when building knowledge-based systems may increase speed and reliability.

An ontology centered on computer attacks was introduced in [16]. That ontology provides a hierarchy of notions specifying a set of harmful actions in different levels of granularity from high level intentions to low level actions. Raskin et al. [17], introduce and advocate the use of ontologies for information security. In arguing the case for using ontologies, they state that ontology organizes and systematizes all of the phenomena (intrusive behavior) at any level of detail, consequently reducing a large diversity of items to a smaller list of properties.

Section – III

Once the Intrusion is confirmed, ontology will be created at Manager based on the attribute defined on the classes of HIDS and NIDS, and if there is new type of attack which is not defined as attribute in class then this new definition of intrusion attack will be added to class of either HIDS or NIDS (depends where it need to be). Following will be the process and class definition. Step 3 and 4 will be same for adding the new definition in signature database and creation of ontology.

6. Process Steps at HIDS

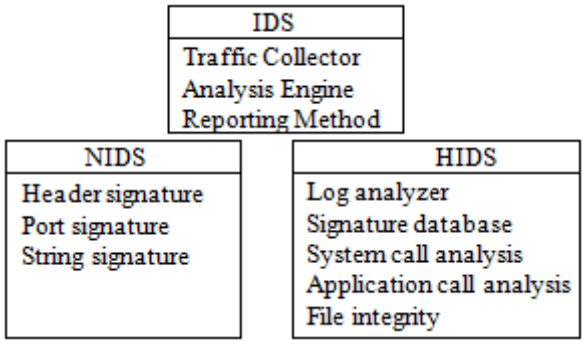
1. Agents working on managed devices send the unsolicited message [SNMP Trap] to Manager.
2. Manager read and analyses for the trap definition for the validity of false negative or false positive.
3. If this is new type of attack for this in signature database, there is no definition, then this definition will be added to signature database else it will be discarded.
4. Immediately after adding the definition of new Intrusion type into the signature database ontology will be created and will send to all the managed devices on the Network.

7. Process Steps at NIDS

1. Manager working on Network management system analyzes the every incoming and outgoing network traffic as per the defined signature database.
2. If manager read and analyses anything which is not matching with defined database then it checks for the possible type of attack.
3. If this is new type of attack for this in signature database, there is no definition, then this definition will be added to signature database else it will be discarded.
4. Immediately after adding the definition of new Intrusion type into the signature database ontology will be created and will send to all the managed devices on the Network.

8. Class definition for IDS, NIDS and HIDS

On the definition of class, we have formed three proposed classes, one is IDS, which has the common sensors of IDS, then two respective classes NIDS and HIDS which are specific to Manager and to Agent devices



9. Ontology Creation

In order to show how the ontology will enables the property on different IDS for determining its state we have taken the help of OWL-DL ontology to describe its top-level hierarchy. The OWL ontology language is based on a family of description logics languages. In particular, OWL-DL is a syntactic variant of the SHOIN (D) description logic [18].

We can define all property like following:

For IDS class

<owl:Classrdf:ID="IDS">
</owl:Class>

<owl:ObjectPropertyrdf:ID="hasTrafficCollector">
<rdfs:domainrdf:resource="#IDS"/>
<rdfs:rangerdf:resource="# TrafficCollector "/>
</owl:ObjectProperty>

<owl:ObjectPropertyrdf:ID="has AnalysisEngine">
<rdfs:domainrdf:resource="#IDS"/>
<rdfs:rangerdf:resource="# AnalysisEngine"/>
</owl:ObjectProperty>

<owl:ObjectPropertyrdf:ID="has ReportingMethod">
<rdfs:domainrdf:resource="#IDS"/>
<rdfs:rangerdf:resource="# ReportingMethod"/>
</owl:ObjectProperty>

In same pattern all attribute of NIDS class can be defined like.

For NIDS class

<owl:Classrdf:ID="NIDS">
</owl:Class>

<owl:ObjectPropertyrdf:ID="hasHeaderSignature">
<rdfs:domainrdf:resource="#NIDS"/>
<rdfs:rangerdf:resource="#HeaderSignature "/>
</owl:ObjectProperty>

<owl:ObjectPropertyrdf:ID="has PortSignature ">
<rdfs:domainrdf:resource="#NIDS"/>
<rdfs:rangerdf:resource="# PortSignature "/>
</owl:ObjectProperty>

<owl:ObjectPropertyrdf:ID="has StringSignature ">
<rdfs:domainrdf:resource="#NIDS"/>

<rdfs:rangerdf:resource="# StringSignature "/>
</owl:ObjectProperty>

For HIDS class

<owl:Classrdf:ID="HIDS">
</owl:Class>

<owl:ObjectPropertyrdf:ID="has LogAnalyzer">
<rdfs:domainrdf:resource="#HIDS"/>
<rdfs:rangerdf:resource="# LogAnalyzer "/>
</owl:ObjectProperty>

<owl:ObjectPropertyrdf:ID="has SignatureDatabase">
<rdfs:domainrdf:resource="#HIDS"/>
<rdfs:rangerdf:resource="# SignatureDatabase "/>
</owl:ObjectProperty>

<owl:ObjectPropertyrdf:ID="has SystemCallAnalysis">
<rdfs:domainrdf:resource="#HIDS"/>
<rdfs:rangerdf:resource="# SystemCallAnalysis "/>
</owl:ObjectProperty>

<owl:ObjectPropertyrdf:ID="has ApplicationCallAnalysis">
<rdfs:domainrdf:resource="#HIDS"/>
<rdfs:rangerdf:resource="# ApplicationCallAnalysis "/>
</owl:ObjectProperty>

<owl:ObjectPropertyrdf:ID="has FileIntregrity">
<rdfs:domainrdf:resource="#HIDS"/>
<rdfs:rangerdf:resource="# FileIntregrity "/>
</owl:ObjectProperty>

Similarly all the classes and there properties can be defined and the property which is just detected for the Intrusion that property can be traced and given send to ontological format to each manager of managed object.

10. Conclusion

The paper presents an idea about how the intrusion detection can be implemented with help of using ontology. After detection is confirmed and if it is not defined how the ontology will be formed. Although we have taken the example of only three classes and few attributes but the real scenario could be entirely different. Ontology will help to communicated and to update the different managers. By this all managers can update their signature database.

11. Future Scope

Discussion on paper concluded on the formation of ontology with OWL-DL language. Intrusion property and there formation and how the property will define the signature syntax and the mapping of SNMP trap values to the property are leaves the further future scope to discuss all this. Further there is a possibility by which we can automate this to monitor system by ontology for all type of attacks.

References

[1] Stallings, W. B., "SNMP, SNMPv2, SNMPv3 and RMON 1 and 2", Third Edition, Addison Wesley Longman Inc., Reading, Massachusetts, 1999.
[2] Microsoft, TechNet, "What is SNMP"http://technet.microsoft.com/en-us/library/cc776379(v=ws.10).aspx
[3] J. Case, M. Fedor, M. Schoffstall, J. Davin, RFC1157 - Simple Network Management Protocol (SNMP), May 1990.
[4] ManageEngine, SNMP Commands, http://www.manageengine.com/network-monitoring/what-is-snmp.html#snmp-basic-commands
[5] Network World, Resource Library, http://www.networkworld.com/details/748.html
[6] M. Rose, "Management Information Base for Network Management of TCP/IP based Internets: MIB II", RFC 1158, May 1980.
[7] Fazelpour, et al. "Management Information Base (MIB) for Open System" DSTC Internal Report, April 1993.
[8] J.P Anderson, Computer Security Threat Monitoring and Surveillance, tech, report, James P. Anderson Co, Fort Washington Pa., 1980.
[9] Intrusion Detection System, http://www.webopedia.com/TERM/I/intrusion_detection_system.html
[10] What is Network Intrusion Detection System, http://www.combofix.org/what-it-is-network-intrusion-detection-system.php
[11] SPANLAWS, How Intrusion Detection System Works, http://www.spamlaws.com/how-intrusion-detection-works.html
[12] Intrusion Detection System, http://www.techotopia.com/index.php/Intrusion_Detection_Systems
[13] Computer Ontology, http://www.techopedia.com /definition /591/computer-ontology
[14] The Semantic Web: "A new form of web content that is meaningful to computers with unleash a revolution of new possibilities"http://www.cs.umd.edu/~golbeck/LBSC690/SemanticWeb.html
[15] Ontologies Advantages, http://mecca.noc.uth.gr/ontologies_advantages.htm
[16] Gorodetski, V. I., Popyack, L. J., Kotenko, I.V., Skormin, V.A.: Ontology-based multi-agent model of information
[17] Security system. In: 7th RSFDGrC. Number 1711 in Lecture Notes in Artificial Intelligence. Springer (1999)
[18] Victor Raskin, Christian F. Hempelmann, Katrina E. Triezenberg, and Sergei Nirenburg. Ontology in information security: A useful theoretical foundation and methodological tool. In Proceedings of NSPW-2001, pages 53 – 59. ACM, ACM, September 2001.
[19] Horrocks and P. F. Patel-Schneider. Reducing OWL Entailment to Description Logic Satis¯ability. Journal of Web Semantics, 1(4), 2004.

Author Profile

Dr. Deo Brat Ojha, PhD from Institute of Technology, Banaras Hindu University, Varanasi (U.P.), India. His research field is Optimization Techniques, Functional Analysis & Cryptography. He

is Professor at Mewar University Chittorgarh, Rajasthan INDIA. He is the author/co-author of more than 250 publications in International/National journals and conferences.

Mr. Vinod Kumar Shukla received the degree of MCA from U.P. Technical University in 2004, has total experience of nine years in teaching and training. He is currently pursuing PhD from Mewar University, Rajasthan, India in the area of Semantic web and Ontology