A Survey on different Ontological Approach and Intrusion Detection System

Mukund Katariya[1], Prof. Tejendra Thakur[2]
[1, 2] Department of Computer Engineering
[1] GTU PG School, Ahmedabad, India
[3] UCET, GTU, India

Abstract- *In information technology, an ontology is a prescribed designation and definition of the categories, properties, and interrelationships of the entities which actually or logically happen for a specific domain of dissertation. Ontologies are a means to logically and fundamentally model that illuminates the structure of a system, i.e., the suitable substances and relations that emerge from its surveillance. Ontology is essentially spawned to explain its elements which are: concepts (classes), instances, individuals or facts, attributes and relations. Intrusion Detection System (IDS) as the name indicates discovers intrusion in the network. It involves both intrusions from intimate and from exterior the network. . In short, IDS is the 'burglar alarm' for the network because much like a intruder alarm, IDS detects the presence of an attack in the network and raises an alert. This paper provides ontological approach for IDS and also provide knowledge based ontological approach.*

Keywords- Ontology, Ontology Languages, IDS, Snort.

I. INTRODUCTION

The word ontology has been recycled in some disciplines, from philosophy, to knowledge engineering. In knowledge engineering ontology is comprised of concepts, concept properties, relationships between concepts and constraints. Ontologies are defined unconventionally from the genuine data and mirror a mutual understanding of the semantics of the domain of dissertation. Ontology is an unambiguous requirement of a representative vocabulary for a domain: definitions of modules, associations, utilities, constraints and other objects. Logically, a reciprocal ontology describes the terminology with which probes and assertions are substituted among software objects. Ontologies are not limited to conventional definitions. Namely, in the traditional logic sense ontology only introduces terminology and does not add any acquaintance about the domain. To specify a conceptualization, we need to formal proverbs that put constraints on the possible explanations for the defined terms.

Ontologies rise out from the division of philosophy known as metaphysics, which works with the environment of actuality – of what arises. This essential branch is anxious with assessingseveralkinds or modes of presence, often with special attention to the dealings between particulars and universals, between core properties and extrinsic properties, between core and existence. The outmodedaim of ontological inquiry in particular is to divide the world "at its joints" to discover those fundamental categories or kinds into which the world's objects naturally fall[1].

In the early 1990s, the widely cited Web page and paper "Toward Principles for the Design of Ontologies Used for Knowledge Sharing" by Tom Gruber [2] is credited with a deliberate definition of ontology as a technical term in computer science. Gruber introduced the term to mean a specification of a conceptualization: ontology is a description (like a formal specification of a program) of the concepts and relationships that can formally exist for an agent or a community of agents. This definition is consistent with the usage of ontology as set of concept definitions, but more general. And it is a different sense of the word than its use in philosophy. [3]

Ontology is an explicit specification of a representational vocabulary for a domain: definitions of classes, relations, functions, constraints and other objects. Pragmatically, a common ontology defines the vocabulary with which queries and assertions are exchanged among software entities. Ontologies are not limited to conservative definitions. Namely, in the traditional logic sense ontology only introduces terminology and does not add any knowledge about the world. To specify a conceptualization, we need to state axioms that put constraints on the possible interpretations for the defined terms. [4]

An IDS is a dedicated tool that identifiesin what manner to describe and interpret network traffic and/or userevents. Therecords can becollected from network packet analysis to the substances of log documents from routers, firewalls, servers, own log of system, network movementdocuments, and more. Additionally, an IDS often save a records of identified attack signatures and it can match patterns of activity, traffic, or elsebehaviour it expresses in the data it's observing against those signatures to identifyat what

time a nearby match between a signature and behaviour occurs. At that time, the IDS make alarms or alerts, and also take some serious actions like shutting down Internet links and/or servers to initiation back-traces, and try to identify attackers and also try for collect evidence of malicious activities by using SNORT.

Snort isanopen source lightweight software for Intrusion Detection System and Prevention System (IDS/IPS). As name suggest it is used to protect the system from attacker. was developed by Martin Roesch with C language in 1998 [5].Snort searches data packet from the traffic and matches with existing rules and/or malicious data traffic. To prevent system from intrusion, IDS-SNORT is used in the form of rules which is in understandable form as per use user can modify it. Snort internally made from Packet Decoder, Pre-processor, Detection engine, Output modules. [6-7]

II. RELATED WORK

Ontology is representing of the particularization of terminology for given domain or module. Logically it provides vocabulary for exchanging of software entities between assertion and probes. On the other hand in conventional ontology methods, it is only provide terminology but it doesn't add any knowledge based work in it. For particular defined terms, it is necessary to update constraints for further interpretation.

Ontology Components: There are two types of components are there one of them is entities of module or domain like concept, relationship, and another one is ontology itself.[8]

Concept: A concept is any experience or function or strategy which later transform in **to** idea. Every sub-concept have main concept.

Relationships: Relationship include is-superclass-of and is-subclass-of. Above relation helps to find which object belongs to from which class object? The is-a relation generate a tree structure. The structure shows relation between objects. How they connected with each other and under which relationship. Second type of relation is part-of which defines how it will combine with other object.

Instances, Individual or fact: Instances, individuals or fact are expressions used to denote elements in the domain. Instances used to denote element for given conception while fact shows relation between hold instances. In domain, any or every element is an Individual which is not class. This is applicable for instances and/or facts.

Attributes: Mainly there are two types of attribute are there: class attributes and instance attributes.

Ontology languages: The author focuses on the different languages, which is used to represent ontology. XML, RDF, RDF-Schema, OWL are the different languages for ontology.[8]

XML (Extended Markup Language): This language is used to describe data in a structured or semi-structured manner. XML language allows user to use number of tags with unsystematic names. The document type definitions (DTDs), is used as key for XML.

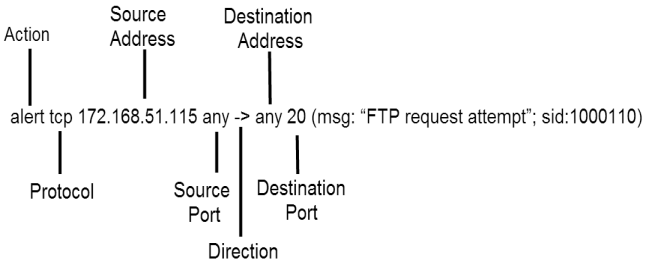
RDF and RDF Schema: Resource Description Framework, as name suggests it is used to locate resources in the form of values, properties and resources. RDFs model is used for formalism of knowledge.

OWL: The combination of RDF / RDF(S) and DAML + OIL has allowed the development of OWL (Web Ontology Language), a standard language for knowledge representation on the Web.

Snort-IDS is a widely used and popular intrusion detection system which provide facility to protect system from intruders and generate alarm. Snort rules have their magical structure which is participate in two logical parts : rule header and rule option.[5-10]

Rule Header	Rule Options

Every rules of SNORT have their magical structure which shown in below example:



An above example of the Snort-IDS rule will generate alert if tcp protocol, source address 172.168.51.115 is detected from any port sent to any destination address and destination port number is 20 (FTP). While in rule option, it will show message like "FTP request attempt" and provide sid: 1000110.[11]

III. COMPARISON OF DIFFERENT TOOLS OF ONTOLOGY

Here below tools are described: Apollo, OntoStudio, Protégé, Swoop and TopBraid Composer (FE). [8-9]

First of all **General description of tool** is shown in Table 1. The table 1 contain information about developer and availability of software, whether software is open source or licence based.

Table 1 General description of the tools

Feature	Apollo	OntoEdit	Protégé	Swoop	TopBraid Composer
Developers	KMI (Open University)	Ontoprise	SMI (Stanford University)	MND (University of Maryland)	TopQuadrant
Availability	Open source	Software license	Open source	Open source	Software license

Software architecture and tool (Table 2) contain necessaryplatforms information which is required to make perfect use of tool. Protégé, OntoStudio andSwoop have client/server architecture, and Swoop is web based architecture. Apollo have file storage ontology and Swoop used as HTML models for storage. Protégé,OntoStudio and TopBraid Composer usagedatabases for storing ontologies.

Table 2 Software architecture and tool evolution

Feature	Apollo	OntoEdit	Protégé	Swoop	TopBraid Composer
Semantic web architecture	Standalone	Eclipse client/server	Standalone and Client-server	Web-based and Client-server	Standalone Eclipse plug-in
Extensibility	Plug-ins	Plug-ins	Plug-ins	Yes Via plug-ins	Plug-ins
Backup management	No	No	No	No	Yes
Ontology storage	Files	DBMS	File and DBMS (JDBC)	As HTML Models	DBMS

Here below in Table 3, **Interoperability** is used to provide interfacebetween different tools and languages for making ontology. This all happening because of integrity.

Table 3 Interoperability

Feature	Apollo	OntoEdit	Protégé	Swoop	TopBraid Composer
With other ontology tools	No	OntoAnnotate, OntoBroker, OntoMat, Semantic and Miner	PROMPT, OKBC, JESS, FaCT and Jena	No	Sesame , Jena and AllegroGraph
Imports from languages	Apollo Meta language	XML(S), OWL, Excel, RDF(S),UML2.0,database schemas (Oracle,MS-SQL, DB2,MySQL), Outlook E-mails	XML(S), RDF(S), OWL, HTML, (RDF,UML, XML)backend, text file, RDF file,Excel, BioPortal and DataMaster	OWL, XML, RDF and text formats	RDFa, WOL, XML(S),RDF(s) ,XHTML, UML, GRDDL, RDB with D2RQ, Microdata and RDFa Web Data Sites, SPIN, Spreadsheets, Oracle database, text file, RDF file, News Feed, Email and Excel
Exports to languages	OCML and CLOS	OWL, RDF(S), RIF, SPARQL, F-Logic and Excel	XML(S), RDF(S),OWL, HTML, Java, Clips, F-Logic SWRL-IQ, Instance Selection, MetaAnalysis, OWLDoc, Queries and (RDF,UML, XML)backend	RDF (S), OIL and DAML	HTML,UML, XSD, Excel , RDB, Oracle database, RDF File, XML File and Text File

Knowledge based representation, Table-4 provide different paradigm between different tools for exchange the knowledge, this approach also known as hybrid representation. OntoEdit provide Onto Knowledge methodology.

Table 4 Knowledge representation and methodological support

Feature	Apollo	OntoEdit	Protégé	Swoop	TopBraid Composer
KR paradigm of knowledge model	Frames (OKBC)	Frames and First Order logic	Frames, First Order logic , SWRL and Metaclasses	OWL	RDF, OWL and SWRL
Axiom language	Unrestricted	Yes (F-Logic)	Yes (PAL)	OWL-DL	OWL-DL
Methodological support	No	Yes (Onto-Knowledge)	No	No	No

In Table-5 which contain **Usability of tools** provide information like graphical taxonomy, graphical views, Ontology library, Collaborative working. As per user ratio Graphical editor Protégé most widely used because it's easy to use, as well as it provide user friendly powerful processing.

Table 5 Usability of tools

Feature	Apollo	OntoEdit	Protégé	Swoop	TopBraid Composer
Graphical taxonomy	No	Yes	Yes	Yes	Yes
Graphical prunes (views)	No	Yes	Yes	No	Yes
Zooms	No	Yes	Yes	No	Yes
Collaborative working	No	Yes	Yes	Yes	Yes
Ontology libraries	Yes	Yes	Yes	No	Yes

IV. CONCLUSION

With emergence of new technology there is need to combine two different domains like Ontology and Snort IDS. With the combination of these two domains we can get all the benefits of both the domain. Users will be able to get different concept easily from knowledge based ontology. This is very useful mechanism for a small scale and medium scale enterprises. In this paper the authors have done the survey and

come up that making ontology for IDS is very useful for knowledge perspective.

REFERENCES

[1] Benjamin, PerakathC.; Menzel, Christopher P.; Mayer, Richard J.; Fillion, Florence; Futrell, Michael T.; deWitte, Paula S.; Lingineni, Madhavi (September 21, 1994). "IDEF5 Method Report" (PDF). Knowledge Based Systems, Inc.

[2] Gruber, T. (1995). "Toward Principles for the Design of Ontologies Used for Knowledge Sharing". International Journal of Human-Computer Studies 43 (5-6):907-928.doi:10.1006/ijhc.1995.1081.

[3] Gruber, T. (2001) "What is an Ontology? ", Stanford University Retrieved 2009-11-09.

[4] J. Cai and V. Eske, "1. Semantic Web: Informational Retrieval System," pp. 1–30.

[5] Snort. Available at http://www.snort.org/snortdownloads?

[6] VinodKumarand Om Prakash Sangwan, "Signature Base Intrusion Detection System Using SNORT," International Journal of Computer Application & Information Technology, pp.35-41, 2012.

[7] Sagar N. Shah and Purnima Singh, "Signature-Base Network Intrusion Detection System Using SNORT And WINPCAP," International Journal of Engineering Research & Technology (IJERT), pp.1-7, 2012.

[8] Emhimed Alatrish,"Comparison Some of Ontology Editors",Management Information Systems, Vol. 8 (2013), No. 2, pp. 018-024

[9] Emhimed Alatrash "Using Web Tools for Constructing an Ontology of Different Natural Languages", Mathematics University of Belgrade.

[10] James Stanger "How to cheat at Securing Linux": Book, Member of Comp TIA's Linux+.

[11] Nattawat Khamphkdee, Nunnapus Benjamas, Saiyan Saiyod"Improving Intrusion Detection System Based on Snort Rules for Network Probe Attack Detection" 2014 2nd International Conference on Information andCommunication Technology (ICoICT).