Semantic Web Based Technique for Network Security Situation Awareness Status Prediction

Pardeep Bhandari[1] , Dr. Manpreet Singh[2]
Doaba College, Jalandhar, India Email: bhandaridcj@gmail.com[1]
Punjabi University, Patiala Email: msgchd@gmail.com[2]

***Abstract*— As the computer network has evolved to provide the user many services, the attacks on these networks to disrupt the services and to gain access to resources has also evolved. New entities in form of services, hardware, network protocols etc. are being added to the network, which is leading to new ways to attack the network. The complexity of the system is increasing so fast that it is becoming increasingly difficult for network administrator to comprehend the situation and react in an appropriate manner. Situation becomes more complex as there is not uniform terminology. Though serious efforts in form of Common Vulnerability Enumeration (CVE), Common Weakness Enumeration (CWE), Common Attack Pattern Enumeration and Classification(CAPEC) etc. has been made, still a long way is to go. In this paper we model a computer network by modelling its components i.e. hardware, software, services using ontology. Also vulnerabilities and attacks on these computers are modelled. We populate our ontology with various instances of vulnerabilities, CVSS scores, attacks and possible services in the network. Knowledge representation methods are used in order to provide Description Logic reasoning and inference over network security status concept. Secondly we propose an ontology based system which predicts probable attacks using inference and information provided by the environment. Results show that proposed method is scalable for large systems and also flexible to incorporate new evolutions in the field of study.**

Index Terms— ***Network security status, ontology, semantic web, SWRL***

I. INTRODUCTION

Computer network is a dynamic entity that evolves over a period of time. New hardware, software, services etc. are deployed and older ones are updated and phased out to match the current requirements of the users. Network Security Administrators are totally dependent on the automated tools to monitor, detect and control the security of the resources of the network and to maintain the availability of the network to the legitimate users. The agents in action in a network and their mutual interaction make it extremely difficult for a network administrator to maintain appropriate level of situation awareness[1][2]. A formal model is required not only to represent entities of a network, but model should be extensible to accommodate new entities and also be able to represent their relationships among the entities. Ontologies have been used to model complex systems also for classification of vulnerabilities, attacks, weaknesses etc. Ontology defines the basic entities of the domain and their relationships using object and data properties. Also it provides rules for combining terms and relations to define extensions to the vocabulary. It represents a particular domain in machine representation and machine processable form.

Tim bass[3] has proposed the concept of Network Security Situational Awareness (NSSA), which tackles the problem of network security with a holistic approach. NSSA is defined as a system that allows network security manager to understand and evaluate the network security holistically. The realization of NSSA is divided into three layers[4]. First is perception of Situational Factors i.e. Situation Perception. Second is evaluation of situation factors (SFs), which involve comprehension, combination, explanation, storage of SFs. The third and most important layer is projection or situation prediction which deals with forecast of the future network security situation. In this paper we propose ontology for second level of NSSA i.e. situation perception i.e. whether network is in safe state, vulnerable state, under attack state. We implement our ontology in web ontology language and make inference using Hermit reasoner. Rules for ontology have been made using Semantic Web Rule Language (SWRL). The paper is structured as follows: In section 2 we define the research problem and the purpose of the paper. In section 3 we discuss related research. In section 4 we present taxonomy of computer network state. In section 5 we propose some rules for extracting the security status of the network. In section 6 we summarize our paper and propose future research directions.

II.RELATED WORK

(Neches,91)(Gruber,93) (Wang J A, Guo M M, Camargo J. (2010) were among the researchers who initially used ontology for specification of a domain in their work. They gave initial guidelines to build ontology. It was earlier effort to support the sharing and reuse of formally represented knowledge among AI systems. Gruber T.R. proposed to write definitions of the concepts of a domain in predicate calculus, which are then translated by a system called Ontolingua in to specialized representation like frame based system and relational languages. [5] proposed use of ontology for definition of detection and reaction process of a security incident. They proposed and ontology based methodology for instantiation of security policy in a particular attack context. For this first alerts are defined and are mapped into particular attack context. After identification of attack, policies to be used to counter the attack are identified using rules. [6] have used ontology in field of intrusion detection. They have proposed ontology specifying a model of computer attack using DARPA- Agent mark-up language and ontology inference layer, which is an extension to Description Logic Language. [7] used ontology for situation awareness. This is one of the earlier efforts to use semantic web in situation awareness. In this landmark paper author represented situation theory of Barwise in terms of OWL ontology. Barwise and Perry gave the earliest formal notion of "situation" to give more realistic formal semantics for speech acts available in their time[20-22]. This paper has highlighted the necessity to develop unambiguous specifications, designs and implementations of situation awareness processes. This research made it possible to represent situation in varied domain in form of semantic web. This is also contribution to the field of information fusion in which data from heterogeneous sources is to be combined. Complex relationships become computer representable and inference becomes possible using reasoners. [8] have proposed a methodology for formal reasoning about situation awareness. In their methodology they have used layered structure for ontology. At the root there is ontology describing minimal set of classes and the important relations between them. In next layer domain specific ontologies are built by inheriting the classes at layer 1. Also domain specific rules are developed that logically describe the condition under which each of the sub-classed relation holds true. These are termed as "Theory of domain". They have substantiated their proposal by representing a battlefield situation. [9] gave a comprehensive survey of the work done in developing taxonomies of attack and vulnerabilities from 1974 to 2006. Idea of this survey was to understand existing attacks and vulnerabilities and to organize the knowledge in form of taxonomy. This can then be used as a framework for detecting similar yet unknown vulnerabilities. (Wang J A, Guo M M, Camargo J. ,2010) built an ontology for vulnerability and proposed an ontological approach to computer system security. Ontology has been used for automated classification of attacks, vulnerabilities, alerts, for specifying of security policies, intrusion detection and reasoning about situation awareness too. [10] have proposed ontology based attack model, which is utilized for security assessment of network and computer system. So use of ontology has been used from different perspectives as shown by above references. Focus of these studies has been to formalize the domain for machine processing so that it may be used for automated classification and detection. Our contribution by current work is to provide the network administrator with context specific assistance in assessment of network security status. Context determines the decision taken by network administrator to counter the security threat being faced by the system. Context of system has been specified in the system in form of the axioms asserted in the ontology.

In this paper we have proposed ontology for defining components of a network. These are hardware, software, which has been further divided into network protocol and services. Various properties have been used for already defined ontologies like CVSS score, attack, actor, attack effect etc. Relationships among these entities have been defined by setting object and data type properties. We implement our ontology into web ontology language (OWL) and make inference by OWL reasoners. After this we used semantic web rule language (SWRL) for specifying rules for interpretation of concepts based upon specific relationship among the entities. Ontology is then populated with sensory inputs as instances. Network Security Status Predictor Simulator has been developed which uses Hermit reasoner to predict security state of the network at any instance.

III. PROPOSED TAXONOMY

In our ontology we have used Hardware, software as base classes from taxonomy proposed by [11]. For attack ontology we have used classes proposed by [12]. Main classes used from this ontology are Actor, Actorlocationl, AttackGoal, AttackMechanism, AutomationLevel, AttackEffect, AttackTarget. Some of the classes originally proposed in the attack ontology have been dropped because of their lesser relevance in current context. Classes Vulnerability, CVSS Score have been picked from CVE schema.

IV. ONTOLOGY PROPOSED

Our ontology has been built based on the taxonomy in the previous section. Top level concepts of ontology include classes mentioned in Fig.1. These are Network, Hardware, Software, Service, Vulnerability, Attack, Attack Effect, Actor Location, Automation Level, Attack Goal , Average Response Time, Average Turn Around Time, CVScore, Service Importance Level, Usage Frequency.

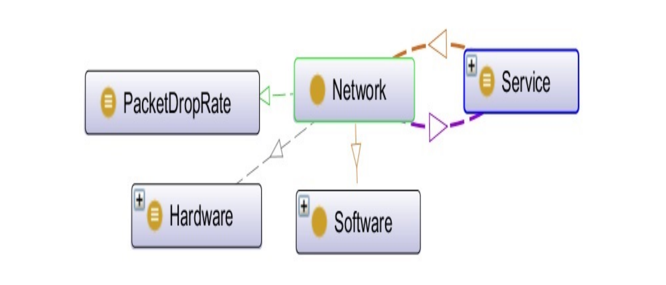


Fig. 2 Network Concept

The concept Network is related with concept hardware and software with properties “NetworkConsistOfHardware” and “NetworkConsistOfSoftware”. Also Network concept is related with PacketDropRate by object property “hasPacketDropRate”. Concept Network is related with concept Service by property “provides” (Fig.2).

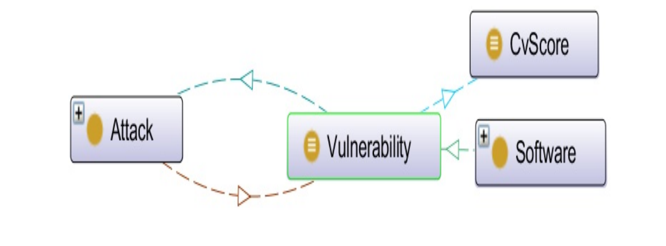
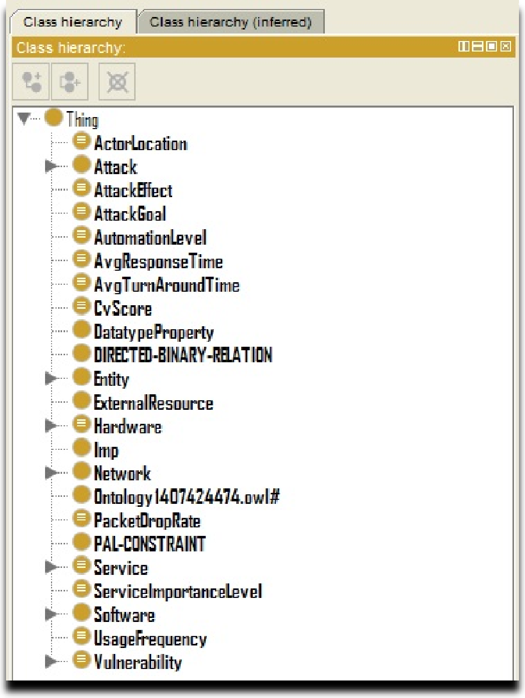


Fig. 3 Vulnerability Concept



Class hierarchy | Class hierarchy (inferred)

Class hierarchy:

- Thing
  - ActorLocation
  - Attack
  - AttackEffect
  - AttackGoal
  - AutomationLevel
  - AvgResponseTime
  - AvgTurnAroundTime
  - CvScore
  - DatatypeProperty
  - DIRECTED-BINARY-RELATION
  - Entity
  - ExternalResource
  - Hardware
  - Imp
  - Network
  - Ontology1407424474.owl#
  - PacketDropRate
  - PAL-CONSTRAINT
  - Service
  - ServiceImportanceLevel
  - Software
  - UsageFrequency
  - Vulnerability

Fig.1 Class Hierarchy

The concept Vulnerability is related with CVScore by object property “hasCVscore” where CVSS is concept adopted from Common Vulnerability Enumeration(CVE) given by mitre.org. CVSS score is common vulnerability scoring system score assigned to every identified vulnerability. The concept Vulnerability is related with concept Attack by property “enables” and with concept Software by property hasVulnerability (Fig.3).

The concept Service(Fig.4) is related with AvgTurnAroundTime, AvgResponseTime, ServiceImportanceLevel, UsageFrequency, ServiceImportanceLevel by properties hasAvgTurnAroundTime, hasAvgResponseTime, hasServiceImportanceLevel, hasUsageFrequency, hasServiceImportanceLevel respectively.

Similarly the concept Attack is related with concept Operating system, AttackEffect, AttackGoal, NetworkProtocol, Hardware, ActorLocation , AutomationLevel by properties hasAttackEffect, hasAttackGoal, targetNetworkProtocol, targetHardware, hasActorLocation, hasAutomationLevel respectively. Table1. Tabulates all the properties and their respective domains and ranges.

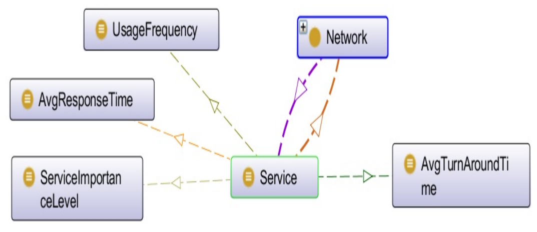


Fig. 4 Service Concept

V. SECURITY ASSESSMENT FRAMEWORK

In this paper, we propose an ontology based framework to assess current security status of the network. Each component of the network is first assessed on the basis of its relationships with other concepts in the ontology. Various scenarios are represented by SWRL rules. The SWRL rule consist of two parts namely antecedent and consequence. Antecedent and consequence consist of conjunction of atoms, which may evaluate to true or false using predicate calculus. The rule implies that if antecedent evaluates to true, then consequence has to be true.

A service provided by the network is inferred to be safe service, vulnerable service or highly vulnerable service depending upon the values of its relationships with other classes namely AvgResponseTime, AvgTurnAroundTime, ServiceImportanceLevel, UsageFrequency and Vulnerability eg. In the following rule Fig.5, a service which has serious vulnerability, very high reponse time, very high turnaround time, high priority importance level and normal usage frequency, is inferred as vulnerable service. Similar rules have been developed for safe service and highly vulnerable service.

VulnerableService(?s) ← SeriousVulnerability(?sv) ∧ Service(?s) ∧ hasAvgResponseTime(?s, VeryResponseTime) ∧ hasAvgTurnAroundTime(?s, VeryHighTurnAroundTime) ∧ hasServiceImportanceLevel(?s, HighPriority) ∧hasUsageFrequency(?s, Normal) ∧ hasVulnerability(?s, ?sv)

Fig. 5 Sample rule to classify Vulnerable Service

Hardware is inferred as SafeHardware or VulnerableHardware depending upon its relationship with class "Vulnerability" by object property "hasVulnerability". Eg. hardware which has a serious vulnerability is asserted to be inferred as vulnerable hardware. Similar rules have been developed for safe hardware.

Vulnerability is inferred to be critical, nominal, serious or no vulnerability depending upon its relation with attack and CVscore concept. Eg. vulnerability which has very high Cvscore and enables a serious attack is inferred as critical vulnerability. Similar rules have been developed for nominal, serious and no vulnerability concepts.

After inferring Hardware, Software, Vulnerability & Service to appropriate categories according to asserted axioms in form of SWRL rules, Network instance is inferred to be in specific state as per its relationship with "PacketDropRate", Hardware, Software and Service through object properties "hasPacketDropRate", "NetworkConsistOfHardware" , "NetworkConsistOfSoftware" , "provides" respectively. Eg. Consider a scenario in which network consists of hardware without vulnerability i.e. safehardware, consists of software with no known vulnerability, has high packet drop rate, provides a highly vulnerable service, such a network is inferred to be a Vulnerable network. Similar rules have been developed for other combinations of service types, hardware types, vulnerability type and values of packet drop.

VI. PREDICTION VIA REASONING (USE CASE)

In this section a use case for evaluating prediction rules is explained. To evaluate the reasoning capabilities of the proposed ontology and knowledge base, we gave current network components and network logs as input. Triples representing simulated logs and events then asserted into the knowledge base. Network is modelled in the ontology by instantiating its software component i.e. network protocol as IPV6, operating system as Window server 2012, hardware components apart from normal peripherals, router deployed is BelkinN900F9k1104V1, service being provided by network are DNS, Email, IRC, VoIP. BelkinN900F9k1104V1 has vulnerability CVE-2012-6371 (3.3,Low) where (CVSS score, severity level). This vulnerability is local network exploitable. Windows 2012 server is known to have vulnerability CVE-2015-1716, CVE-2015-1702, CVE-2015-1699 and CVE-2015-1698. These vulnerabilities have CVSS score and severity as (5.0, Med.), (6.9, Med), (9.3, High) and (9.3, High) respectively. Moreover CVE-2012-6371 i.e. vulnerability in router is known to be local network exploitable, so actor location is local. IPV6 has vulnerability CVE-2014-0254(7.8, High). The observed packet drop rate in the network is "high packetdrop rate". These facts are modelled in the ontology through instance creation. Reasoner is called to check concept consistency, detect duplicates and infer types of each of the new instance based upon chain of implications of SWRL rules asserted in the ontology knowledgebase. Fig.6 shows the rules used to mark the state of network as the Vulnerable Network.Unlike traditional methods like taxonomies or attack languages, the technique of using ontology and SWRL makes the system maintainable and easy to update for new components in the system whether hardware or software, new services and new vulnerabilities which are published may be represented in the system.

- Vulnerability(?v) ∧ Attack(?a) ∧ hasCVscore(?v, lowCVscore) ∧ enablesAttack(?v,?a) -> NominalVulnerability(?v)
- Vulnerability(?v) ∧ Attack(?a) ∧ hasCVscore(?v, highCVscore) ∧ enablesAttack(?v,?a) -> SeriousVulnerability(?v)
- Vulnerability(?v) ∧ Attack(?a) ∧ hasCVscore(?v, veryhighCVscore) ∧ enablesAttack(?v,?a) -> CriticalVulnerability(?v)
- Attack(?a) ∧ hasActorLocation(?a, LocalActor) ∧ hasTargetNetworkProtocol(?a, IPV6) ∧ hasAutomationLevel(?a, Automatic)-> SeriousAttack(?a)
- Software(?s) ∧ Vulnerability(?v) ∧ hasVulnerability(?s,?v) -> VulnerableService(?s)
- Hardware(?h) ∧ hasVulnerability(?h, ?v) -> VulnerableHardware(?h)
- Network(?n) ∧ Software (?s) ∧ Hardware(?h) ∧ Service(?s) ∧ NetworkConsistofSoftware(?n, ?s) ∧ NetworkConsistofHardware(?n?h) ∧ provides(?n, ?s) ∧ hasPacketDropRate(?n,highPacketDropRate)-> VulnerableNetwork

Fig. 6 Chain of rules used to predict Network Security Status

VII. EVALUATION OF ONTOLOGY

For evaluation of ontology following metrics taken from[13] have been used

1. Quantitative Evaluation: These metrics are divided into two groups viz. Ontology Metrics and Knowledge Base Metrics

i. Ontology Metrics

a. Object Property Richnesss=
(No. Of Object Property + No. Of Datatype property)/ All properties including is-a relationship=31/46=0.67
b. Inheritance Richness = (No. Of subclasses/ No. Of classes)=18/16=1.125
c. Data Properties Richness =
(No. Of functional object properties/ No. Of classes) = 12/16=0.75

ii. Knowledge Base Metrics :

a. Class Richness =

(No. Of Non-empty class i.e. class with individual)/No. Of classes=34/34=1

b. Class Connectivity = The connectivity of a class (*Conn*(*Ci*)) is defined as the total number of relationships instances of the class have with instances of other classes. It is to be calculated for each class individually. Table.2 shows that Network, Vulnerbility and Attack are most connected classes of the ontology.

c. Class importance

The Table.3 shows that Network and Vulnerability have emerged to be most important classes, which is true as practically vulnerability always leads to the attacks in the network.

VIII. CONCLUSION

Ontology and SWRL driven approach in the field of network security is a promising approach. The experiments have shown this technique to be scalable, flexible and updatable to adapt to new challenges being faced in network security domain. New concepts introduced in the domain may easily be added to the existing system, thus making them easily updatable. Flexibility is the commendable feature of the approach as the system may be tuned to different domains and tolerance levels as per network administrator's requirement by assertion of appropriate rules in the system. To improve its utility and applicability, informal knowledge in the natural language sources could be extracted from various informal sources using natural language processing techniques.

REFERENCES

[1] P. Bhandari,M.Singh , "Ontology based approach for perception of network security state," *2014 Recent Adv. Eng. Comput. Sci.*, pp. 1–6, Mar. 2014.

[2] C. Onwubiko, "Functional requirements of situational awareness in computer network security," *2009 IEEE Int. Conf. Intell. Secur. Informatics*, pp. 209–213, 2009.

[3] T. Bass, "a glimpse into the future of id," pp. 1–10, 2009.

[4] Z. Yong, T. Xiaobin, and X. Hongsheng, "A Novel Approach to Network Security Situation Awareness Based on Multi-Perspective Analysis," *2007 Int. Conf. Comput. Intell. Secur. (CIS 2007)*, pp. 768–772, Dec. 2007.

[5] J. E. L. De Vergara, E. Vázquez, A. Martin, S. Dubus, and M.-N. Lepareux, "Use of Ontologies for the Definition of Alerts and Policies in a Network Security Platform," *J. Networks*, vol. 4, no. 8, pp. 720–733, Oct. 2009.

[6] J. Undercoffer, A. Joshi, and J. Pinkston, "Modeling Computer Attacks : An Ontology for Intrusion Detection," pp. 113–135, 2003.

[7] M. M. Kokar, C. J. Matheus, and K. Baclawski, "Ontology-based situation awareness," *Inf. Fusion*, vol. 10, no. 1, pp. 83–98, 2009.

[8] C. J. Matheus, K. Baclawski, and M. M. Kokar, "Derivation of ontological relations using formal methods in a situation awareness scenario," no. April, pp. 298–309, 2003.

[9] N. Of, "COMMUNICATIONS T AXONOMIES OF A TTACKS AND," pp. 6–19, 2008.

[10] J. Gao, B. Zhang, X. Chen, and Z. Luo, "Ontology-based model of network and computer attacks for security assessment," *J. Shanghai Jiaotong Univ.*, vol. 18, no. 5, pp. 554–562, Oct. 2013.

[11] S. Hansman, S. Engineering, and N. Zealand, "A Taxonomy of Network and Computer Attack Methodologies," 2003.

[12] R. van Heerden, L. Leenen, and B. Irwin, "Automated classification of computer network attacks," *2013 Int. Conf. Adapt. Sci. Technol.*, pp. 1–7, Nov. 2013.

[13] A. P. Sheth, "Ontological evaluation and validation," 2003.

SNO.	PROPERTY NAME	DOMAIN	RANGE
1.	NetworkConsistOfHardware	Network	Hardware
2.	NetworkConsistOfSoftware	Network	Software
3.	HasPacketDropRate	Network	Packetdroprate
4.	provides	Network	Service
5.	hasCVscore	Vulnerability	CVScore
6.	Enables	Vulnerability	Attack
7.	hasVulnerability	Software, hardware	Vulnerability
8.	hasAvgTurnAround Time,	Service	Avgturnaroundtime
9.	hasAvgResponseTime,	Service	Avgresponsetime
10.	hasServiceImportanceLevel,	Service	Serviceimportancelevel
11.	hasUsageFrequency,	Service	Usagefrequency
12.	hasServiceImportanceLevel	Service	Serviceimportancelevel
13.	hasAttackEffect,	Attack	Attackeffect
14.	hasAttackGoal,	Attack	Attackgoal
15.	targetNetworkProtocol,	Attack	Networkprotocol
16.	targetHardware,	Attack	Hardware
17.	hasActorLocation,	Attack	Actorlocation
18.	hasAutomationLevel	Attack	Automationlevel
19.	Isprovidedby	Service	Network
20.	Enabledby	Attack	Vulnerability

Table 1. Object Properties in ontology

SNo.	Class	No. of relationship with other classes
1.	Network	4
2.	Vulnerability	3
3.	Hardware	2
4.	Software	2
5.	Service	5
6.	Attack	8
7.	Avgresponsetime	1
8.	Avgturnaroundtime	1
9.	Automationlevel	1
10.	Attackeffect	1
11.	Actorlocation	1
12.	Serviceimportancelevel	1
13.	Usagefrequency	1
14.	CVscore	1
15.	Attackgoal	1
16.	Packetdroprate	1

Table 2. No. of relationships per class

SNo.	Class	Class Importance
1.	Network	0.433
2.	Vulnerability	0.107
3.	Hardware	0.087
4.	Software	0.033
5.	Service	0.073
6.	Attack	0.040
7.	Avgresponsetime	0.020
8.	Avgturnaroundtime	0.020
9.	Automationlevel	0.020
10.	Attackeffect	0.027
11.	Actorlocation	0.020
12.	Serviceimportancelevel	0.027
13.	Usagefrequency	0.013
14.	CVscore	0.027
15.	Attackgoal	0.033
16.	Packetdroprate	0.020

Table 3 Class Importance