A Qualitative Analysis of An Ontology Based Issue Resolution System for Cyber Attack Management

Chris B. Simmons, Sajjan G. Shiva
Computer Science Department
University of Memphis
Memphis, Tennessee
{cbsmmons, sshiva}@memphis.edu

Lakisha L. Simmons
Management of Information Systems
Belmont University
Nashville, Tennessee
lakisha.simmons@belmont.edu

***Abstract*—Cyber-attacks are increasing at an alarming rate and the attackers have progressively improved in devising attacks towards specific targets. To further develop the area of cyber-attack communication, we propose an ontology based issue resolution system used to identify and defend against cyber-attacks. The issue resolution system (IRS) facilitates attack discovery and suggestive defenses for a small to medium sized organizations. We validate our IRS Ontology using qualitative study of security expert professionals and highlight future work intended to simulate the IRS in a virtual attack test environment.**

***Index Terms*—Issue Resolution System, Attack Ontology, Security, Management**

I. Introduction

Cyber-attacks have created a global threat to local and global networks. Attacks are becoming more sophisticated and possess the ability of spreading in a matter of seconds. It is essential to provide tools necessary in detecting, classifying, and defending against attacks. An ontology is a common way to organize knowledge and involves the description of objects and relationships [1], thus enabling a mechanism for attack incident and response. Standard ontologies classify vulnerabilities, computer and network attacks, security threats, and events. Current security ontologies are limited by ontology construction frameworks, such as OWL, RDF, and DAML, to name a few. We build upon ontologies through the use of a cyber-attack taxonomy, wherein attack vectors are used to capture the path an attacker utilizes to gain access. Amer and Hamilton [2] stated that a complete secure solution considers more than one aspect. A broad view of an attack is essential for various personnel, but providing a holistic approach for the entire organization highlighting attack details is pertinent to ensure appropriate classification and communication.

Typically, organizations question the impact a cyber-attack has once its target is compromised. One approach to gaining insight into the attacker's target is to consider the attack paths, or combination of exploits [3]. This paper presents a guide intended primarily with aiding an organization decipher attack characteristics and implement a communication mechanism as cyber incidents are made available for analysis and defense. At a high level, our main contribution solicits security expert knowledge to develop an improved cyber-attack ontology for classification and communication. This holistic approach facilitates the classification of attack vector information, which considers vulnerabilities or any means by which an attack exploits to conduct an attack. This ontology does not provide information to determine if the attack is successful, but rather classifies the attack vectors to gain insight for appropriate countermeasures. When applied within a knowledge management capacity, the ontology is beneficial to management, network administration, development, test, and support personnel.

In this paper, we present an intuitive approach using an ontology based issue resolution system (IRS). The IRS utilizes AVOIDIT [4], an enhanced cyber-attack taxonomy, as a solution addressing the deficiency in existing taxonomies. The IRS is intended to provide a defender with attack vector details to what encompasses an attack and any impact the attack may have on a targeted system. The use of the IRS provides a repository to label attack vector information as it is stored using an iterative process. The tree like structure is formalized using information extraction and data mining techniques to display the complete attack path within the issue resolution system. We provide a prototype implementation of the issue resolution system capturing web application data in a virtual environment. Our security expert interview results show that the IRS ontology provides intuitive concept relationships for a functional system usage.

This paper is organized as follows: In Section II we survey existing security related ontologies and knowledge based systems. In Section III, we highlight our methodology in which the security expert interviews were conducted for the development of our cyber-attack ontology. In Section IV, we present the proposed IRS Ontology. In Section V, we provide the corpus development in which the IRS was populated with common vulnerabilities and exposures. In Section VI we highlight the IRS rules created from expert interviews with an intuitive example. In Section VII, we provide an implementation the Ontology within the IRS to demonstrate its utility, as well as the IRS Experiment in Section VIII. In Section IX, we conclude this paper followed by future work in Section X.

II. Related Work

Ontology is a common way to organize knowledge and involves the description of objects and relationships [1]. Furthermore, ontologies provide a mechanism for shared vocabularies, which allow an improvement of information retrieval, and assist data integration [5]. Generally speaking, an ontology captures explicit knowledge used for concepts and

relationship building to infer implicit knowledge. An ontology can include terms originated using defined rules and properties. Ontologies are the core component to the development of knowledge systems and domain modeling of the environment in terms of labeled concepts and relationships. They are intended to provide knowledge engineers with reusable knowledge for problem-solving methods and reasoning services [6].

There are several methodologies that highlight ontology development within various disciplines. Methonology is an ontology building methodology that focuses on the reuse or reengineering ontologies [7].The CO4 project involves a methodology that builds upon incremental knowledge being integrated into a knowledge base formally and informally [8]. The KACTUS project involves a methodology that builds upon itself as knowledge grows during each application being implemented [9]. The On-To-Knowledge methodology involves gathering project objectives through four steps kickoff, refinement, evaluation, and ontology maintenance that are used within a knowledge management tool [9]. Although, this research is not focused on the knowledge gained by the development of applications and projects, a focal point is placed on the knowledge gained from each discovered use of an attack vector and associated information.

Cheah [8] described the need of multi-site project management (MSPM), where a need for an ontology that best suites this knowledge as software development is becoming a multi-site initiative. OWL was used to conceptualize the knowledge specifications into logical data models. Jarrar et al. [10] proposed using conceptual data modeling techniques for building ontologies. This provided an ontology-engineering framework that enables reusing conceptual models for modeling and representing ontologies. Guarino [11] explored the strong connection between knowledge engineering, conceptual modeling, and formal ontologies to enhance the emerging field of ontology engineering. This research involving the development of ontologies assisted with the baseline for the development of the IRS Ontology.

Foley and Fitzgerald [12] proposed a semantic threat graph approach to autonomously manage security policy configuration associated with enterprise threats. In this work the semantic threat graph is used in the form of an ontology to represent enterprise assets and countermeasures associated to threats. Foley and Fitzgerald extend taxonomic hierarchical type threat trees to produce the semantic threat graph providing a more explicit threat depiction relative to semantic knowledge of low-level security configurations.

D'Amico et al. [13] presented a mission critical ontology used to provide asset relationship with users in the event of a cyber-attack. This work was composed at a workshop derived from the Camus project, in which security experts within the commercial sector and military were surveyed using situational cyber analysis to develop the mission critical ontology. This work was developed in aspirations to further research in regards to security knowledge elicitation or assist organizations with scenario analysis.

Mulwad, et al. [14] proposed a framework for extracting unstructured information from text within external repositories, such as CVE, CCE, CPE, CVSS, OVAL, etc. This work uses Wikitology for its ontology conceptual model of cyber incidents and a computer security taxonomy from Wikipedia to classify vulnerabilities.

There is an increased complexity pertaining to the data storage of cyber attack information and its systematic approach to managing information. As knowledge management is a continuous developing field that remains full of research methodologies to capture knowledge. Andrade and Saltz proposed a knowledge base management system that provides the capability of using an ontology-aware database management system [15]. This technique is useful as it provides a repository store framework for capture and dissemination of information. Dalkir [16] proposed techniques used to elicit tacit knowledge codification within an organization using cognitive maps, decision trees, and knowledge taxonomies. Codification of knowledge allows the collection of knowledge to be shared and used within an organization. This provides good insight to constructing our ontology to ensure critical relationships are provided to capture knowledge beneficial for reuse.

III. IRS METHODOLOGY

The development of an user interface will require eliciting relevant knowledge from security experts in the field to distinguish vital content when assessing a cyber incident and the development of the issue resolution system. Ransbotham and Mitra [17] provide insight into a conceptual model of paths to information security compromise, in which security experts are elicited for experiential knowledge in relaton to organizational security investment. Our interview consisted of seventeen (17) open-ended questions related to what security professionals described as being an important need of an informative security management system for cyber-attack classification and resolution. The interviews were conducted with IT Security professionals such as Vice President of Security Firm, Senior Security Analysts, Quality Assurance Analysts, Computer Scientists, and Security Wireless Network Engineers. The professionals were from 5 small-to-medium businesses, 3 governmental entities, and 2 educational professionals.

To date, ten (10) interviews have been completed, which provided insight to where organizations see cyber security management and potential areas of focus in the dispersing cyber incident information. This work contributes to the computer security field through updating the cyber security terminology and its association to cyber threat classification and response. Questions were asked based on the literature above discussing discovery, reporting, and countermeasures when a potential attack is discovered. In the results section we provide a summary of each question from each professional. Table III in the appendix consists of the questions that were asked to the security professionals.

IV. IRS Ontology

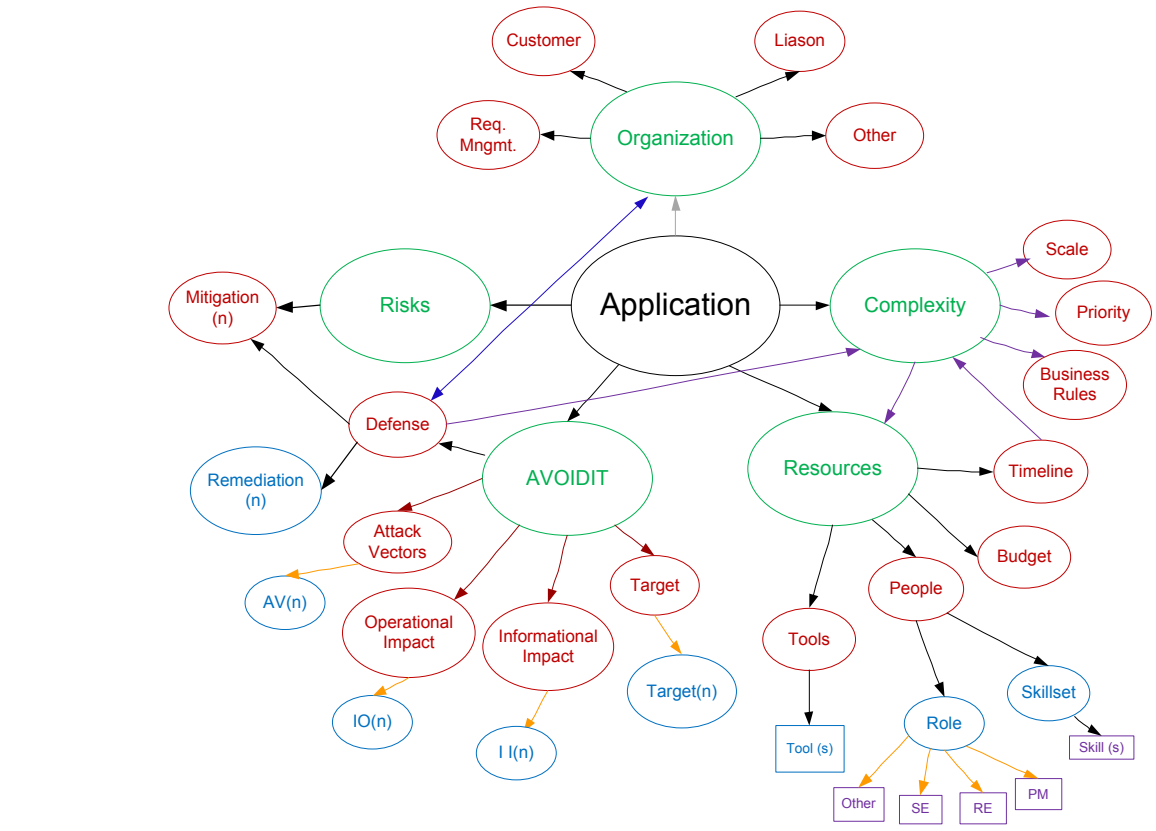
Wang and Guo [18] stated a heavy-weight ontology may be considered a formal logic system, which includes rules, concepts, concept taxonomies, relationships, properties, axioms and constraints.

The IRS was developed for small and medium sized organizations to improve communication and reuse of defenses until the attack has been mitigated and/or remediated. Figure 1 provides an overview of IRS ontology to support comprehending communication flow within an organization upon attack discovery. The objective of the security ontology is to provide knowledge representation of the most relevant security concepts within an organization. Gruber [6] has provided a set of criterion to ensure best the developed ontology is useful, which are: (i) clarity, (ii) coherence, (iii) extendibility, (iv) minimal encoding bias, and (v) minimal ontological commitment.

Figure 1 highlights the IRS ontology to support the communication flow within an organization upon attack discovery. The objective of the security ontology is to provide knowledge representation of the most relevant security concepts within an organization. The **ovals** refer to major concepts that are needed to successfully communicate an incident within the IRS. The **boxes** refer to the terminal entities that provide specifics of the superclass concepts. The **arrows** refer to the relationships between concepts relevant to incident management.

The top level concepts branching out from the center of the IRS application are: (a) AVOIDIT Taxonomy, (b) Risks, (c) Organization, (d) Complexity, and (e) Resources. For brevity we discuss the top-level concepts

IRS Ontology



associatedWith – who assigns a task
has/have – information needed to complete superclass. The direction is one-way.
is – an option associated with a higher level concept.
consistOf – is the superclass concept that contains vital subclass relationship.
approvedBy – who approves
influencedBy – the associated impact

Fig. 1. IRS Ontology

A. AVOIDIT Taxonomy

Simmons, et al. [4] provided the AVOIDIT cyber-attack taxonomy to support comprehending each attack classification and how a variety of attacks are represented in each category. Using AVOIDIT incidents classified via attack vectors where the repository disseminates the potential attack for an appropriate defense selection. AVOIDIT couples defenses within an attack taxonomy to understand the exploit and derive strategies needed to prevent auxiliary damages. Due to space constraints, the AVOIDIT Taxonomy was omitted.

B. Risks

The risks concept enables an organization to understand the risks that are involved with a particular application. Upon the discovery of a cyber incident and no defense solution exists, the mitigation strategy is used to determine the impact of minimizing the risk until a solution has been developed.

C. Organization

The organization concept provides a means in which to communicate with management and respective stakeholders relative to an incident. This entity has approval ownership of the application currently being monitored for cyber incidents.

D. Complexity

The complexity relates to the intricacy of the cyber incident and how long before mitigation and/or remediation takes place. This provides insight to how difficult the cyber incident is relative to the organization's level of importance in defending against the incident, as well as creating and following business policies.

E. Resources

The resources concept within the IRS ontology provides an understanding of who has ownership over the day-to-day operations involving the cyber incident, as well as the capability of responding to the potential breach. This ensures the appropriate personnel are in direct communication involving the cyber incident.

V. Corpus Development (Populating the IRS)

The anonymous cyber-attacks, as well as the purported China cyber-attacks, on various U.S. governmental agencies have placed cyber-attacks at the forefront. The World Economic Forum has established cyber-attacks as a global risk within its 2013 Global Risk report [19]. Utilizing an issue resolution system application aids the need for educating cyber defense in an expected future of cyber warfare.

A knowledge system harnesses tacit knowledge from subject matter experts and prior data to create a system where information is transferred throughout the organization. The basis of an IRS provides a resource in capturing information relative to the business environment and engineer knowledge suitable for transfer. Knowledge systems for knowledge engineering have been studied extensively, but remains limited regarding cyber security. The corpus was first developed by selecting various common vulnerabilities and exposures (CVEs) associated to open source applications. The second stage imported prepared excel spreadsheets to be used in the corpus for analysis. To build the corpus the CVEs were converted to excel format for importing into the IRS. The CVEs from the National Vulnerability Database (NVD) containing incidents relative to open source applications were used as the basis of the corpus. Table I depicts a Joomla! CVE description, which highlights the vulnerability information.

TABLE I. CVE Description of Joomla! CVE-2011-4804

CVE -2011-4808	
Summary	SQL injection vulnerability in the HM Community (com_hmcommunity) component before 1.01 for Joomla! allows remote attackers to execute arbitrary SQL commands via the id parameters in a fnd home action to index.php.
Published	12/14/2011
CVSS Severity	7.5 (High)

VI. IRS Rule Creation and Example

We utilize the knowledge engineering extracted from the security experts to solidify concept relationships associated to cyber incident communication. The security experts were given separate CVEs from the National Vulnerability Database (NVD) and interviewed regarding the important factors of a CVE and its associated connection within an organization. Currently, there exist two major rules created to extract security incident information from the CVEs. The rules were created in pseudo code for clarity and programmed into the IRS. The security experts identified the classification accuracy, risk factors, whether the software is in use, and the historical performance. The pseudo code was then programmed into the IRS to extract information for each major rule. In order to ensure IRS extracts useful information, security experts who regularly analyze common vulnerability and exposures provided their analysis of relevant information of interest.

Results of the expert interviews revealed that the experts were interested in the following categories of security incidents (1) whether the incident involves software in use (2) accurately classified incident (3) the risk factors associated to the incident (4) historical performance. The highlighted categories made up the two sets of information extraction rules. Simmons [20] utilized a similar strategy to extract pertinent information from business reports. Rule 1 denotes the software incidents and its respective cause and results if the incident is successful. Rule 2 intuitively provides the organization a high level view of the type of vulnerability extracted from a CVE present in the vulnerable application. See Table II for the four sets of extraction rules.

TABLE II. CVE Information Extraction Major Rule Sets

1. A rule to identify software incidents	***for*** each row in the portion of the CVE from which we want to extract information ***if*** the keyword is a candidate indicating a software incidents within an organization (e.g., Joomla, Wordpress, Drupal) ***then*** return the keyword noun phrase

	and return verb phrase immediately following the keyword and present them software incidents (e.g. verb phrases-allow, allows)
	if keyword is a verb phrase denoting cause (e.g. disabled)
	then return the verb phrase and following noun phrases as reasons
	if keyword is a verb phrase indicating result (e.g. read, execute, inject, include)
	then return the verb phrase and following noun phrases as results
	
	end if
	end for

2. A rule to identify vulnerability	***for*** each row in the portion of the CVE from which we want to extract information
	if the keyword is a candidate indicating a vulnerability incident within an organization (e.g., SQL Injection, XSS, Directory Traversal)
	then return the keyword phrase
	and return the phrase immediately following the keyword and present them as cyber incident
	end if keyword noun phrase is software keyword (e.g. Joomla, Wordpress, Drupal)
	
	end if
	end for

Now, let us consider an organization running an online booking PHP based application connected to a MySQL server database. An incident is discovered by the defender, wherein an attacker is attempting to assess the MySQL server using a SQL injection vulnerability via an online booking application. The defender is able to view the SQL injections attempts via the web server log file. The defender uses the national vulnerability database to see if any new incidents have been reported, however it will take the defender a significant amount of time to discern if a fix is available.

The IRS provides an ontological representation of the cyber incident and the communication involved to educate the defender of the current state of the system. It uses pull technology to bring the information to the defender without having to search for suggestive countermeasures. Continuing our example, using the IRS, the SQL Injection vulnerability targets a vulnerability in a PHP application version 3.2, which has a defense influenced by a high complexity. The IRS identifies that a CVE does not exist and uses historical data to determine the defense as Block IP address, until a fix has been established. Therefore, the Defense is *influenedBy* the Complexity of the SQL Injection vulnerability. The Complexity is also *influencedBy* the Resources available to defend or repair the vulnerability, pending *approvalBy* the sales organization. Once the AVOIDIT portion of the ontology is populated with the necessary vulnerability information, the IRS communicates within the entire organization for proper allocation of resources and approvals. This offers a framework for organizational awareness and its impact when a cyber incident has taken place. We illustrate the necessary IRS concepts using figure 2.

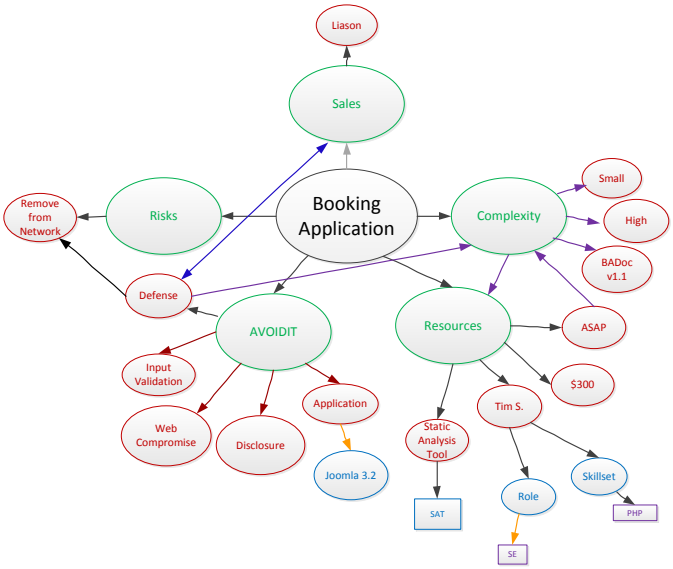


Fig. 2. IRS Ontology Example

VII. IN Y

The IRS is used as a discovery and dissemination tool involving attack data and defenses. The IRS achieves these goals by using AVOIDIT as the basis for its repository schema to classify the entire path of an attack. IRS is not an intrusion detection system, but works together with an IDS. Once the attack characteristics are determined, the attack is identified and the IRS is used to obtain additional information pertaining to that attack and defense policies. IRS is intended for small and medium sized organizations to improve communication and reuse of defenses until the attack has been mitigated and/or remediated.

The IRS will be implemented using an open-source development tools, such as PHP as the scripting language and MySQL as the database. Codeigniter [21] is used as our knowledge base interface. Figure 3 depicts our proposed IRS where a user is able to view reports involving hourly, daily, and monthly incidents, related to attack vectors and view attack trees of potential attacks.

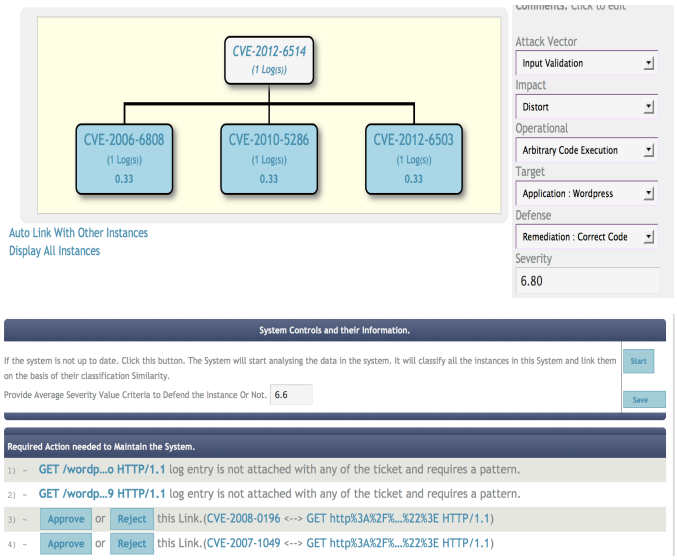


Fig. 3. IRS User Interface

AVOIDIT applied within the IRS provides a common way to represent security knowledge for an entire organization to benefit in all disciplines. Figure 3 highlights a vulnerability within the IRS and its ability to link tickets representative of attack vectors in a tree structure. This enables the IRS to display to the defender the alternative and complete paths of an attack. As we view figure 3, let us consider support personnel, being the first-line of assistance to the users, with a common understanding of security when logging information of incidents that will benefit during knowledge transfer. The network administrators will have the initial information to mitigate and/or remediate the incident without spending a considerable amount of time to gain understanding. Using the IRS provides the ability for knowledge to transfer seamlessly correlating previous, current, and future attacks. The IRS provides a more apparent approach to educate the defender on attack vectors used to launch attacks. Moreover, the IRS allows the entire organization and key stakeholders to stay abreast of the current state of their monitored applications. This improves efficiency when protecting against cyber attacks.

VIII. IRS Experiment Setup

We set up the IRS in a virtual attack test environment as highlighted in Figure 4. The test environment consists of the Ubuntu based UltimateLAMP VMWare image containing multiple vulnerable web applications, such as Joomla, Drupal, and dotProject. The test environment also consists of the Metasploitable Ubuntu 8.04 server install on a VMWare 6.5 image, which mainly consists of networking vulnerabilities. Figure 4 depicts an attack against a Joomla web application. We use the Metasploit [22] joomla_tinybrowser module to conduct the attack and exploit a vulnerability in Joomla 1.5.12 tinybrowser plugin. This particular attack is used to perform a file upload and execute arbitrary code on the targeted system. This Metasploit module connects to the target server and allows the attacker to upload a file without logging in. Once successfully connected to the server an attacker modifies the file name to prevent detection with the option to conduct further damage.

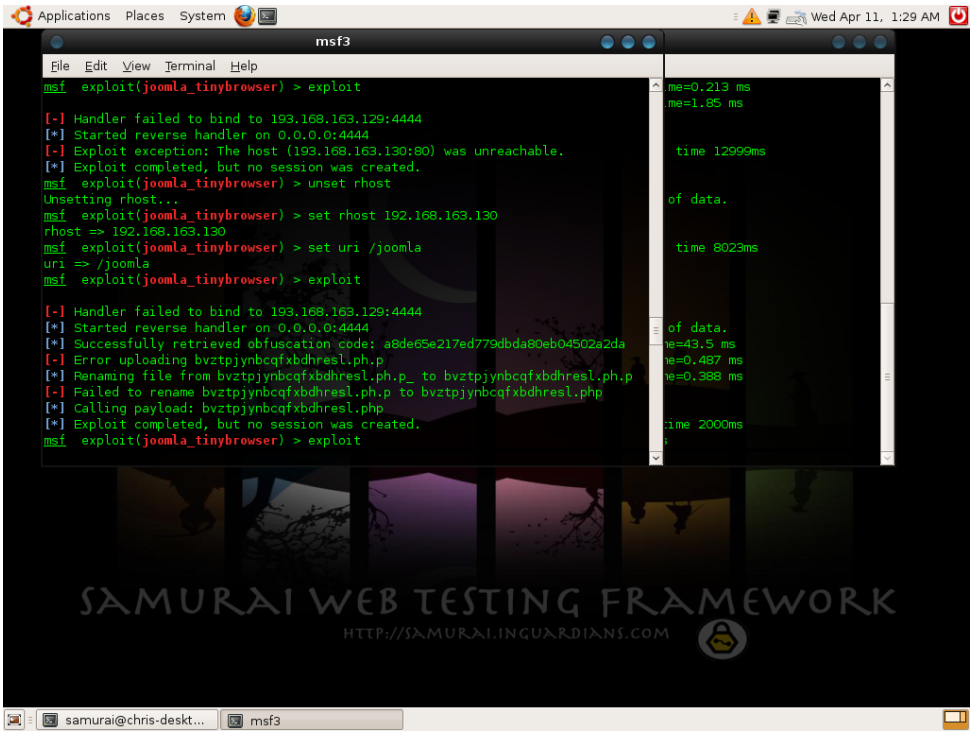


Fig. 4 .Virtual Machine Test Environment

We use the IRS within this test environment, as illustrated above, to assist with classifying pertinent discovery information towards defense notification prior to a full attack. We conduct multiple attacks using Metasploit attack modules against various web applications associated with the following external cyber vulnerabilities:

- CVE-2007-4184 (Base Score 7.5) – **Joomla!**
- CVE-2006-4234 (Base Score 7.5) – **dotProject**
- CVE-2008-3886 (Base Score 4.3) – **dotProject**
- CVE-2006-6808 (Base Score 6.8) - **Wordpress**
- CVE-2006-2667 (Base Score 7.5) - **Wordpress**

Conducting this task allows the assessment of the IRS and its ability to discover attack data and disseminate applicable defenses within the organization. In a preliminary experiment, we utilized 500 CVEs to test the IRS's capability of classifying vulnerability information. The IRS successfully retrieved 443 specific CVEs associated to Wordpress. Of the 443, 414 were correctly classified using the knowledge levied by security experts. A recall/true positive rate of ninety-three percent (93%) was exhibited. This is reflective of a system

providing the administrator pertinent information associated to the systems of interest. Figure 5 highlights the associated CVEs retrieved by the IRS relative to the application installed.

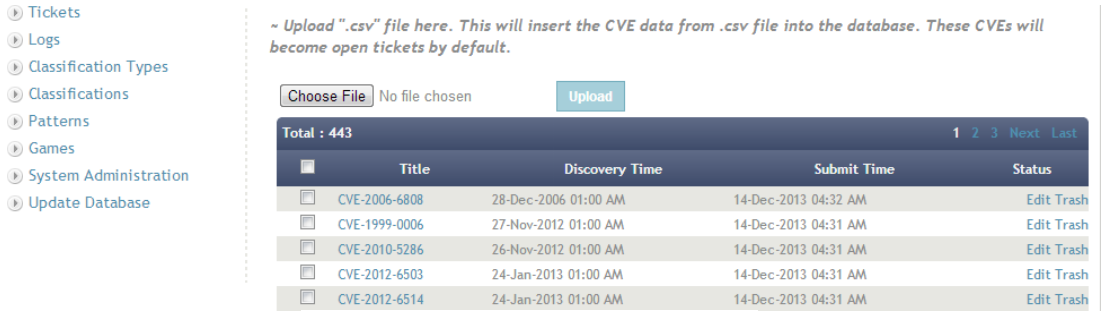


Fig. 5. IRS User Interface

Future work is in progress to correlate application log instances from our test environment with CVE information to afford a system administrator the capacity of quickly mitigating problematic instances in a system, and prevent subsequent attack vectors. The highlighted CVEs and their respective applications will be used for testing purposes.

IX. Conclusion

This paper provides an ontology-based issue resolution system that classifies attack vector information to facilitate communication within the organization. This communication will provide a holistic view of required personnel and resources to effectively advise and construct defense strategies relative to cyber incidents. It is essential as cyber-attacks continue to evolve that a knowledge system matures in capturing significant attack data to improve an organization's resiliency. Using the security expert interviews we have created and programmed intuitive rules into the issue resolution system to pinpoint the classification of vulnerabilities, attacks, and security threats to benefit cyber security awareness in an organization. In the initial version of this prototype we only used CVEs from an external repository containing attack vector information that were found in the National Vulnerability Database. This paper aims to increase an organization's attack acumen in all functional areas, as opposed to specific individuals.

X. Future Work

This paper is proposed to continuously evolve the dynamics of ontology-based systems with respect to cyber security. Further development is ongoing in the development of our issue resolution system, where an AVOIDIT schema will be used to enumerate and classify attack vector discovery for optimal defense. Figure 3 and 5 depict our proposed IRS where a user is able to view reports related to attack vector information and view attack trees of potential attacks. Work is in underway regarding the correlation of application logs from our test environment with CVE information to allow an administrator the ability mitigate cyber related events in a web application.

Further, we will use the issue resolution system within a Game Inspired Defense Architecture (GIDA) [23] to investigate the applicability of the ontology-based IRS to classify attack vector information in determining the action space of the attacker. The IRS will determine the type of attack. GIDA will use the information to assess candidate game models identified by the IRS to select the optimal game model for defense [24]. The architecture consists of a game assessment system where we demonstrate the assessment of candidate game models which can be used for defending against a particular kind of attack. This assessment can be used to identify the game model which is most relevant to the attack in question and hence be executed by our proposed model to yield a better overall payoff to the defender.

References

[1] Tran, Quynh-Nhu Numi, and Graham Low. "MOBMAS: A methodology for ontology-based multi-agent systems development." *Information & Software Technology* 50, no. 7/8 (June 2008): 697-722.

[2] Amer, S., Hamilton, J. "Intrusion Detection Systems (IDS) Taxonomy – A Short Review". Defense Cyber Security, 13 (2), June 2010.

[3] Noel, S., Jajodia, S., O'Berry, B., Jacobs, M. "Efficient Minimum-Cost Network Hardening via Exploit Dependency Graphs". in Proceedings of the 19th Annual Computer Security Applications Conference, Las Vegas, Nevada, December 2003.

[4] Simmons, C., Shiva , S., Dasgupta , D., and Wu, Q., "AVOIDIT: A cyber-attack taxonomy,", Technical Report: CS-09-003, University of Memphis, August 2009.

[5] J. Euzenat, Corporative memory through cooperative creation of knowledge bases and hyper-documents, in: Proc. 10th Knowledge Acquisition for Knowledge-Based Systems Workshop (KAW96), Banff, 1996.

[6] T. Gruber. Towards Principles for the Design of Ontologies used for Knowledge Sharing. International Journal of Human-Computer Studies, 1995. 43(5/6): 907-928.

[7] M. Fernandez-Lopez, A. Gomez-Perez, A. Pazos-Sierra, J. Pazos-Sierra, Building a chemical ontology using METHONTOLOGY and the ontology design environment, IEEE Intelligent Systems & their applications 4 (1)(1999) 37–46.

[8] Cheah, C. "Ontological Methodologies – From Open Standards Software Development to Open Standards Organizational Project Governance" *IJCSNS International Journal of Computer Science and Network Security*, VOL.7 No.3, March 2007.

[9] J. Euzenat, Corporative memory through cooperative creation of knowledge bases and hyper-documents, in: Proc. 10th Knowledge Acquisition for Knowledge-Based Systems Workshop (KAW96), Banff, 1996.

[10] Jarrar, M., Demey, J., and Meersman, R. "On using conceptual data modeling for ontology engineering", *Journal on Data Semantics* 2800: 185–207, 2003.

[11] Guarino, N, "Understanding, building and using ontologies*," International Journal of Human Computer Studies*, 1997. **46**: pp. 293-310.

[12] S. N. Foley and W. M. Fitzgerald, "Management of Security Policy Configuration using a Semantic Threat Graph Approach," *Journal of Computer Security (JCS)*, vol. 19, 2011.

[13] A. D'Amico, L. Buchanan, J. Goodall, and P. Walczak. Mission Impact of Cyber Events: Scenarios and Ontology to Express the Relationships between Cyber Assets, Missions and Users. International Conference on Information Warfare and Security, April 2010.

[14] V. Mulwad, W. Li, A. Joshi, T. Finin, and K. Viswanathan, "Extracting Information about Security Vulnerabilities from Web Text," Web Intelligence for Information Security Workshop. IEEE Computer Society Press, August 2011.

[15] Andrade, H. and Saltz, J. "Towards a knowledge base management system (KBMS): An ontology-aware database management system (DBMS)"*Proceedings of the 14th Brazilian Symposium on Databases*, Florianopolis, Brazil.

[16] Dalkir, K. (2005) "Knowledge Management in Theory and Practice - Knowledge Capture and Codification," Elsevier. Butterworth-Heinemann, Burlington, MA.

[17] Ransbotham, S., Mitra, S. "Choice and Chance: A Conceptual Model of Paths to Informaiton Security Compromise," *Information Systems Research*, 20(1) 121-139, 2009.

[18] Wang, J.A., Guo, M. "OVM: An Ontology for Vulnerability Management." CSIIRW '09, April 13-15, Oak Ridge, Tennessee, USA.

[19] The Global Information Risk Report. available at www.weforum.org/reports, Retrieved January 5, 2013.

[20] Simmons, Lakisha. "Extraction of Ontology and Semantic Web Information from Online Business Reports," PhD Dissertation, University of Mississippi, 2011.

[21] Codeigniter. Retrieved January 18, 2013. http://ellislab.com/codeigniter .

[22] Metasploit Framework User Guide. Version 2.5., http://metasploit.com/projects/Framework/docs/userguide.pdf, retrieved September 6, 2011.

[23] S. Shiva, H. Bedi, C. Simmons, M. Fisher, R. Dharam. Holistic Game Inspired Defense Architecture, International Conference on Data Engineering and Internet Technology, March, 2011.

[24] Sajjan Shiva, Harkeerat Singh Bedi, Chris Simmons and Vivek Shandilya (2012) A Game Inspired Defense Architecture. Poster presented at the Third Conference on Decision and Game Theory for Security, Budapest, Hungary, November 5-6, 2012.

APPENDIX: QUESTIONS FOR SECURITY EXPERTS

This section provides the questionnaire that was used to conduct the security expert interview. Table III highlights the questions that were presented to the security experts.

TABLE III. SECURITY EXPERT QUESTIONNAIRE

Discovery	What is the common vulnerability exposure (CVE) report number you have selected?
	Using the provided CVE report, please provide terms that are useful when distinguishing an attack.
	Does the CVE present a complete path to an attack?
	Do you believe there are distinct paths to information security compromises?
	Generally, do attack paths progress from information gathering (probes) to targeted attacks? [1]
Reporting	What pertinent data would you use in reporting a security incident?
	How would you determine if the data presented in the CVE is relevant to your organization?
	What factors would you use to distinguish the level of importance within a CVE?
	What are the factors that you identify when determining a security breach within your organization is of high importance?
Countermeasures	What managerial, organizational, and environmental factors lead to better countermeasures within an organization? [1]
	What managerial factors can reduce an attacker's attraction toward a targeted system? [1]
	What are organizational consequences of information security compromise? [1]
General Questions	Are there any further details you believe should be mentioned relating to discovering, reporting, or countering attacks?
	Do you believe there is a necessity to develop a system to assist those less familiar with security breaches?

	Are there any systems you believe will assist a novice with understanding various aspects of security breaches?
	With your understanding of security, do you believe the current security terms capture a complete picture to successfully transfer knowledge within an organization?
	Does the Ontology depicted provide an appropriate organization of information relevant to security?