

Ontology-Based Decision Support for Security Management in Heterogeneous Networks

Michał Choraś^{1,2}, Rafał Kozik², Adam Flizikowski^{1,2}, Rafał Renk^{1,3},
and Witold Hołubowicz^{1,3}

ITTI Ltd., Poznań
Institute of Telecommunications, UT&LS Bydgoszcz
Adam Mickiewicz University, Poznań
michal.choras@itti.com.pl, chorasm@utp.edu.pl, holubowicz@amu.edu.pl

Abstract. In this paper our original methodology of applying ontology-based logic into decision support system for security management in heterogeneous networks is presented. Such decision support approach is used by the off-network layer of security and resiliency mechanisms developed in the INTERSECTION Project. Decision support application uses knowledge about networks vulnerabilities to support off-network operator to manage and control in-networks components such as probes, intrusion detection systems, Complex Event Processor, Reaction and Remediation. Hereby, both *IVO* (Intersection Vulnerability Ontology) as well as *PIVOT* - decision support system based on the vulnerability ontology are presented.

1 Introduction

INTERSECTION (INfrastructure for heTERogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks) is a European co-funded project in the area of secure, dependable and trusted infrastructures. The main objective of INTERSECTION is to design and implement an innovative network security framework which comprises different tools and techniques for intrusion detection and tolerance.

The INTERSECTION framework as well as the developed system called IDTS (Intrusion Detection and Tolerance System) consists of two layers: in-network layer and off-network layer. Our decision support system is placed in the off-network layer of the INTERSECTION security-resiliency framework. The role of the off-network decision support system is to support network operators in controlling complex heterogeneous and interconnected networks and real-time security processes such as network monitoring, intrusion detection, reaction and remediation.

The knowledge about vulnerabilities is needed to more effectively cope with threats and attacks, and to understand interdependencies and cascade effects within the networks. Therefore network vulnerabilities should be identified, described, classified, stored and analyzed. The framework operator should be able to control in-network processes and trigger/stop their reactions on the basis of

the vulnerability knowledge which is incorporated in our decision support system intelligence by means of the vulnerability ontology.

In this paper we show, how the previously described concept of INTERSECTION Vulnerability Ontology in [1][2][3] is now used for decision support. The paper is structured as follows: ontology-based approach is introduced and motivated in Section 2. Our vulnerability ontology is presented in Section 3. Decision support application based on ontology is described in Section 4.

2 Vulnerability Knowledge for Decision Support - Ontology-Based Approach

In both computer science and information science, an ontology is a form of representing data model of a specific domain and it can be used to e.g.: reason about the objects in that domain and the relations between them. Since nowadays, we can observe the increasing complexity and heterogeneity of the communication networks and systems, there is a need to use high-level meta description of relations in such heterogeneous networks.

This need and requirement is particularly apparent in the context of Future Internet and Next Generation Networks development. From operators point of view, two important issues concerning communications networks are: security and Quality of Service.

In the past years critical infrastructures were physically and logically separate systems with little interdependence. As digital information gained more and more importance for the operation of such infrastructures especially on the communication part. Communication part of critical infrastructures are the one of the most important part that represents the information infrastructure on which critical infrastructures rely and depend.

The communication part is typically related to telecom operators or separate department inside company that manages the network. The last decade has seen major change in telecommunication market in most of European countries.

The are two main factors that cause those changes:

- Market deregulation that enables new telecom providers to enter the market
- New technologies and solutions that cause lower costs of services, introduction of the new services and increased telecom traffic.

Unfortunately, the increasing complexity and heterogeneity of the communication networks and systems increase their level of vulnerability.

Furthermore, the progressive disuse of dedicated communication infrastructures and proprietary networked components, together with the growing adoption of IP-based solutions, exposes critical information infrastructures to cyber attacks coming from the Internet and other IP based networks.

To deal with those problems there is a need to create good information security management system that will allow the administrators to deal with a great amount of security information and make the decision process effective and efficient.

To support those tasks we propose to develop the security framework consisting of several modules as well as of the decision support system based on the applied ontology.

3 Ontology Design

One of the goals of the INTERSECTION project is to identify and classify heterogeneous network vulnerabilities. To match this goal we have proposed a vulnerability ontology. The major aim of our ontology is to describe vulnerabilities beyond single domain networks and to extend relations/restrictions onto heterogeneous networks. Our ontology is now called *IVO* - INTERSECTION Vulnerability Ontology.

Networks vulnerabilities tend to be often mistaken with threats and attacks. Therefore we decided to clearly define vulnerability as asset-related network weakness. Obviously, then such weaknesses are exploited by threats and attacks. Such vulnerability definition is based on ISO/IEC 13335 standard and is shown in Figure 1 [4].

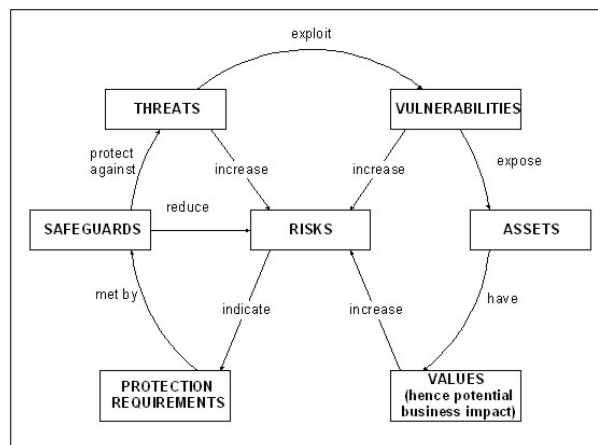


Fig. 1. Vulnerabilities identification and definition on the basis of networks assets

Networks assets should also be defined and described. We decided to use Shared Information/Data (SID) Model in which networks assets and relations between them are defined. SID Model provides Physical Resource Business Entity Definitions [5]. SID assets description is specified in UML and visualized using UML diagrams.

In our ontology approach, we found Resources and Vulnerabilities classes as the most important components. Class Resources is based on division proposed in SID (Shared Information/Data Model).

It includes following subclasses:

- Physical Resources,
- Logical Resources,
- Software
- Service.

Class Vulnerabilities is connected with Resources (exposed by them). That is why subclasses of Vulnerability class are:

- Physical Resources Vulnerabilities,
- Logical Resources Vulnerabilities,
- Software Vulnerabilities.

Every subclass inherited properties and restrictions from its superclass that is why we decided to classified our ontology in this way. For example classes Wired and Wireless inherited Resources, Topology, Vulnerabilities, Network Structure, Risk and Safeguards from superclass Network.

Our vulnerability ontology is focused on network design vulnerabilities (e.g. protocols weakness etc.). In contrast there are some implementation vulnerabilities, however these are already stored in National Vulnerability Database (*NVD*) [6].

4 Ontology Applied to Decision Support

The created ontology is applied in our decision support system intelligence providing knowledge about vulnerabilities and how they influence specific interconnected scenarios.

Decision support system applied to security management in heterogeneous networks has the following functionalities:

1. Provides information about influence of heterogeneity onto networks security and resiliency issues
2. Provides information to Intrusion Detection and Anomaly Detection Systems decision support tool provides information about security risks and threats in particular scenarios (what networks are interconnected, what technologies are used etc.). Intrusion detection systems receive information on how to act in such scenarios (e.g. how often the packets should be sniffed, what features should be extracted etc.)
3. Supports decisions of Intrusion Tolerance Systems decision support system provides information about tolerance, expected False Positives etc.
4. Provides useful information for security architecture visualization module additional information for end-users (network management operators)
5. Supports Complex Event Processor Module (a part of IDS system) - decision support drives the decision engine while performing the correlation activity
6. Decision support system cooperates with the relational vulnerabilities database (*IVD*) created in FP7 INTERSECTION Project.

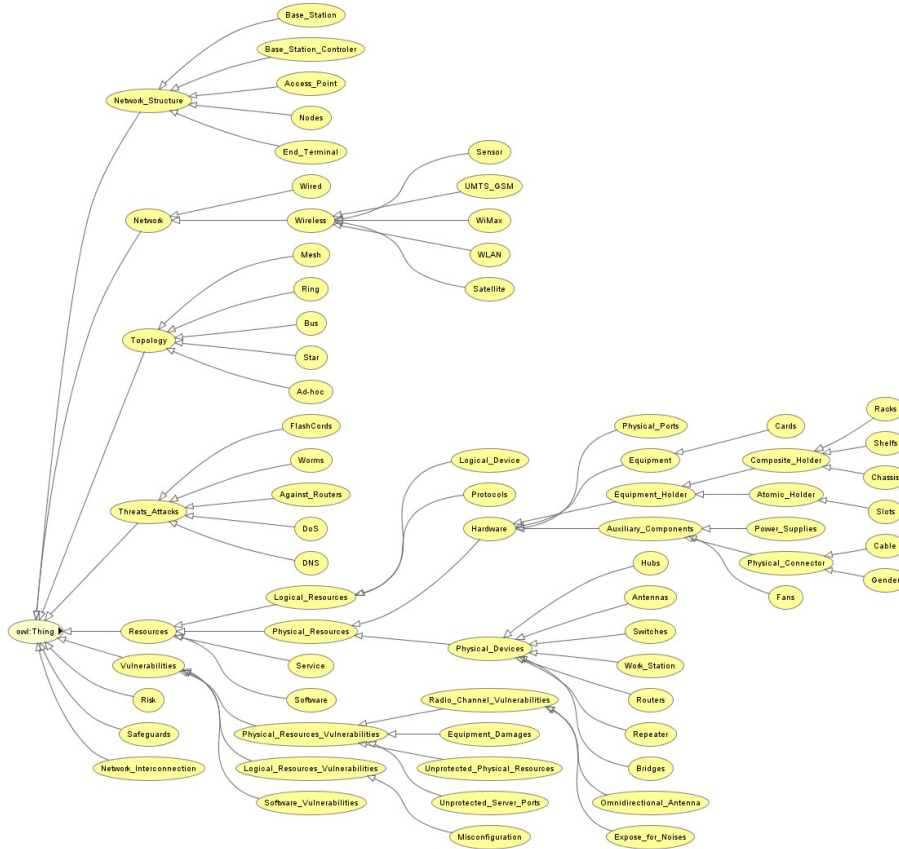


Fig. 2. IVO Visualized in Protege

PIVOT (Project INTERSECTION Vulnerability Ontology Tool) is the ontology-logic based decision support tool. Our goal was to apply ontology in a real-life decision-support application.

It is end-user oriented application, which allows to modify and browse the vulnerability ontology. One of the biggest advantages is tool has client-server architecture, what allows to share one ontology by multiple users (e.g. by network operators).

The ontology interface built in PIVOT is user-friendly and intuitive.

The application consists of MySQL storage database, Protege OWL API, Tomcat WWW server and OpenLaszlo framework. The backbone of the tool is Protege API. It is an open-source Java library for the Web Ontology Language and RDF(S).

The API provides classes and methods to load and save OWL files, to query and manipulate OWL data models, and to perform reasoning. Furthermore, the API is optimized for the implementation of graphical user interfaces. The

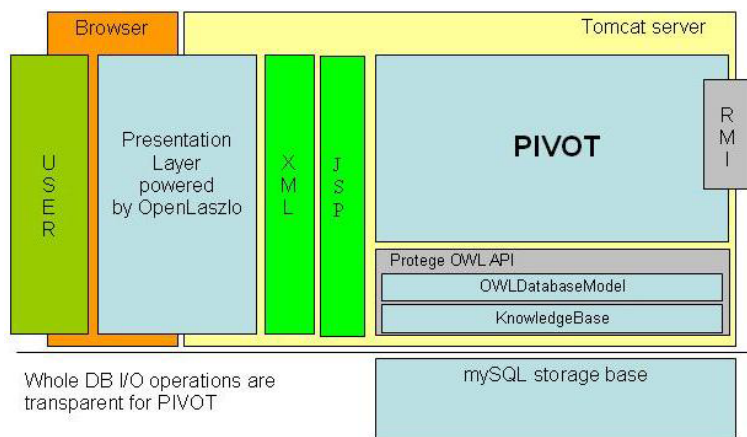


Fig. 3. PIVOT architecture

greatest part of API is that Protege allows to work with OWL model having MySQL database in backend, what makes dramatic performance improvements.

Client-server architecture allows to share one ontology model with multiple users. Each connection to PIVOT is transactional, what provide better ontology database integrity. All database operation (the way the model is stored in db) are transparent for PIVOT, what means that user do not have to worry about establishing connection, committing changes (made on model) or bothering where and how the particular instance is stored.

Actual version of PIVOT allows to establish two types of connection - the RMI and the HTTP. RMI (Java Remote Method Invocation API) is a Java application programming interface for performing the remote procedure calls. This type of PIVOT interface was developed to be use with other components in local network. This gives opportunity to share ontology among other processes running on remotes machines.

The HTTP interface is developed to perform easy OWL model maintenance and management through the web browser. This functionality is provided by Apache Tomcat server. This server is developed by the Apache Software Foundation (ASF). Tomcat implements the Java Servlet and JavaServer Pages (JSP) specifications form Sun Microsystems, and provides a pure Java HTTP web server environment for Java. It is used as a PIVOTs module which is started on PIVOT boot up.

Java Server Pages (JSP) is Java technology that allows software developers to dynamically generate HTML, XML or other types of documents in response to web client request. The technology allows Java code and certain predefined actions to be embedded into static content. PIVOT benefits from easy XML document generation. This format allows to define own elements and to help share structured information via network, what makes PIVOT more universal.

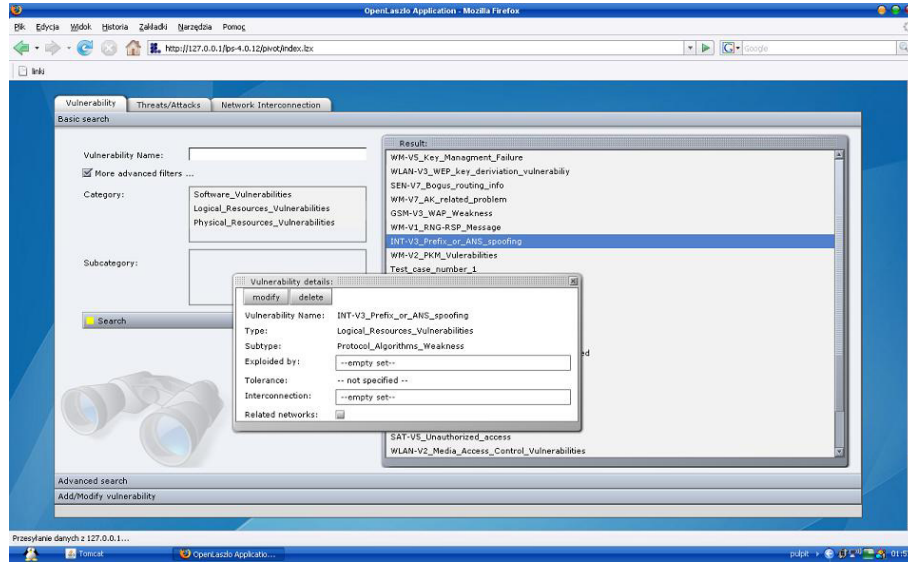


Fig. 4. PIVOT in operation (screenshot)

To boost the presentation layer OpenLaszlo is used. It is an open source platform for the development and delivery of rich Internet applications.

PIVOT architecture is presented in Figure 3.

PIVOT is now available at: <http://193.142.112.119:8081/lps-4.1.1/pivot/>. PIVOT interface in operation is shown in Figure 4.

5 Conclusions

The major contribution of this paper is a new approach to vulnerability description and handling based on the ontology logic. INTERSECTION Vulnerability Ontology has been motivated and presented in detail. We also showed how to apply *IVO* in an innovative decision support system used in INTERSECTION security-resiliency framework. Moreover, PIVOT - ontology-logic based decision support application has been developed and presented.

Our decision support system can be used by end-users such as networks operators and telecoms to manage heterogeneous and interconnected networks.

Acknowledgement

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement no. 216585 (INTERSECTION Project).

References

1. FP7 INTERSECTION Deliverable D.2.2: Identification and classification of vulnerabilities of network infrastructures (2008)
2. Flizikowski, A., et al.: On Applying Ontologies to Security and QoS Management in Heterogeneous Networks. In: Information Systems Architecture and Technology - Information Systems and Computer Communications Network, 189-200, ISBN 978-83-7493-416-9 (2008)
3. Michal, C., et al.: Ontology-based description of networks vulnerabilities. Polish Journal of Environmental Studies 5c (2008)
4. ISO/IEC 13335-1:2004, Information Technology Security Techniques Management of information and communications technology security Part 1: Concepts and models for information and communications technology security management
5. Shared Information/Data Model TeleManagement Forum (2002)
6. <http://nvd.nist.gov/>
7. FP7 INTERSECTION (INfrastructure for heTErogeneous, Reislent, Secure, Complex, Tightly Inter-Operating Networks) Project Description of Work.
8. Ekelhart, A., et al.: Security Ontologies: Improving Quantative Risk Analy-sis. In: Proc. of the 40th Hawaii International Conference on System Sciences (2007)
9. <http://protege.stanford.edu/>
10. OWL Web Ontology Language Semantics and Abstract Syntax (2006), <http://www.w3.org/TR/owl-features/>
11. SWRL: A Semantic Web Rule Language Combning OWL and RuleML, W3C Member Submission, <http://www.w3.org/Submission/SWRL/>
12. Spector, A.Z.: Achieving application requirements. Distributed Systems, 0-201-41660-3, 19-33 (1990)
13. Gomez, A., Corcho, O.: Ontology languages for the Semantic Web. IEEE Intelligent Systems 1904, 54-60 (2002)