INTERSECTION APPROACH TO VULNERABILITY HANDLING

Michał Choraś[1,3], Salvatore d'Antonio[2], Rafał Kozik[3] and Witold Hołubowicz[4]
[1] *ITTI Ltd., Poznań, Poland*
[2] *Consorzio Interuniversitario Nazionale per l'Informatica CINI, Naples, Italy*
[3] *Institute of Telecommunications, University of Technology & Life Sciences, Bydgoszcz, Poland*
[4] *Adam Mickiewicz University, Poznań, Poland*

Keywords: Network security, Heterogeneous network, Vulnerability database, Ontology management, INTERSECTION.

Abstract: In this paper our approach to heterogeneous networks vulnerability handling is presented. Vulnerabilities of heterogeneous networks like satellite, GSM/GPRS, UMTS, wireless sensor networks and the Internet have been identified, classified and described in the framework of the European co-funded project, named INTERSECTION (INfrastructure for heTErogeneous, Resilient, SEcure, Complex, Tightly Inter−Operating Networks). Since computer security incidents usually occur across administrative domains and interconnected networks it is quite clear that it would be advantageous for different organizations and network operators to be able to share data on network vulnerabilities. The exchange of vulnerability information and statistics would be crucial for proactive identification of trends that can lead to incident prevention. Network operators have always been reticent to disclose information about attacks on their systems or through their networks. However, this tendency seems to be overcome by the new awareness that it is only through cooperation that networking infrastructures can be made robust to attacks and failures. Starting from these considerations, we developed two components, namely INTERSECTION Vulnerability Database (IVD) and Project INTERSECTION Vulnerability Ontology Tool (PIVOT), for vulnerability data management and classification. Both tools will be presented in this paper.

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. The in-network layer is a distributed system comprising a number of components aiming at detecting and tolerating intrusions in real-time and automated fashion, while the role of the off-network layer 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 enhance networks security. Therefore network vulnerabilities should be identified, described, classified, stored and analyzed. To achieve these goals, a vulnerability database and vulnerability ontology are required. The framework operator should be able to control in-network processes and trigger/stop their reactions on the basis of the vulnerability knowledge provided by vulnerability ontology and vulnerability repository. Therefore, both vulnerability database and vulnerability ontology are developed and implemented within the INTERSECTION security-resiliency system.

In this paper we focus on presenting off-network layer components devoted to handling network vulnerabilities. In Section 2 INTERSECTION Vulnerability Database will be presented. In Section 3 ontology-based approach to handle identified vulner-

ChorÅąs M., dâĂŹAntonio S., Kozik R. and HoÅĆubowicz W.
INTERSECTION APPROACH TO VULNERABILITY HANDLING.
DOI: 10.5220/0002790601710174
In *Proceedings of the 6th International Conference on Web Information Systems and Technology (WEBIST 2010)*, page
ISBN: 978-989-674-025-2

abilities will be shown. The practical aspects of both components offered to project end-users will be provided.

2 INTERSECTION VULNERABILITY DATABASE

One of the INTERSECTION framework components is the vulnerability database, which stores the information about design vulnerabilities of heterogeneous and interconnected networks.

Design vulnerabilities differ from implementation vulnerabilities (i.e. application faults) on which *NVD* (National Vulnerabilities Database) is focused. The INTERSECTION Vulnerability Database (*IVD*) is based on the *CVE* (Common Vulnerabilities and Exposures) vulnerability naming standard and uses the following *SCAP* (Security Content Automation Protocol) standards:

- Common Configuration Enumeration (*CCE*)
- Common Platform Enumeration (*CPE*)
- Common Vulnerability Scoring System (*CVSS*)

The Common Configuration Enumeration provides common identifiers to system configurations in order to facilitate fast and accurate correlation of configuration data across multiple information sources and tools. *CCE* is primarily used to identify security related configuration issues. The Common Platform Enumeration is a structured naming scheme for information technology systems, software, and packages. Finally, the Common Vulnerability Scoring System is an open standard for assigning a score to a vulnerability that indicates its relative severity compared to other vulnerabilities.

The use of such standards enables automated vulnerability management, measurement, and policy compliance evaluation and allows the INTERSECTION vulnerability database to interoperate with other databases, such as *NVD* (National Vulnerability Database) and *OSVDB* (Open Source Vulnerability Database).

The INTERSECTION Vulnerability Database is accessible by end-users, such as telecom providers and network operators, via web browser.

IVD enables most of standard database functionalities (browsing, querying), however some of the functionalities are available for registered users only.

The database is composed of the following main tables:

- Vulnerability,
- *CVSS*,
- *CCE*,
- Network Asset,
- Solution.

Vulnerability table contains information about discovered vulnerabilities. The type of vulnerability, the threats and attacks exploiting the vulnerability, the discovery date and the likelihood of the vulnerability are some of the attributes used to describe a vulnerability. *CVSS* table provides an overall *CVSS* score for each identified vulnerability. Base metrics and temporal metrics defined by the *CVSS* standard are employed in this table to score the impact of each vulnerability. *CCE* table provides information about network system mis-configurations which generate a vulnerability. The mis-configuration is specified by means of values of specific configuration parameters. Technical mechanisms to get the correct values of such parameters are also described. Network Asset table is used to provide information about network platforms, systems, and devices affected by vulnerabilities. Finally, solution table contains a description of the patches, solutions, and countermeasures which are recommended to fix a vulnerability.

The INTERSECTION Vulnerability Database is available at: $http://192.167.9.116:81/ivd/$.

3 VULNERABILITY HANDLING - 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. There are two main factors that cause those changes:

- market deregulation enables new telecom providers to enter the market
- new technologies and solutions lower costs, new services, increase telecom traffic.

This provides to create many different networks that uses different technologies and equipment that have to cooperate each other. 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. From the telecom provider point of view the security and dependability of their network and IT systems depends on two main factors security and dependability of their own solutions and interconnections to other.

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 applied ontology.

3.1 Intersection Vulnerability Ontology - IVO

One of the goals of the INTERSECTION project is to identify and classify heterogeneous network vulnerabilities (0). 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.

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 (0).

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 (0). SID assets description is specified in UML and visualized using UML diagrams.

In our ontology approach, we found Resources and Vulnerabilities classes as a 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.

We propose to apply ontology into the security-resiliency framework. Ontology knowledge and PIVOT (Project INTERSECTION Vulnerability Ontology Tool) are crucial elements of the off-network part of the INTERSECTION framework (so called off-network Intrusion Detection Tolerance System).

In our understanding, to successfully apply the created ontology, the following elements have to be taken into account:

- Classes and their attributes with restrictions (created in *OWL* (0))
- Rules for these classes and attributes (created in *SWRL* (0))
- Instances stored in a related relational database.

To apply the ontology, restrictions and rules are crucial without them ontology would not be functional.

3.2 Ontology-based Tool - PIVOT

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

PIVOT is designed to be serve transactional operations over single ontology model. To accomplish this goal transactional SQL database is adopted to store ontology model and make dramatic performance improvements during I/O operations. Transactional provide also better ontology model integrity. Client-server architecture allows to share one ontology model with multiple users.

PIVOT basic functionalities:

- Searching vulnerabilities matching prompted criteria
- Adding, modifying ontology instances
- Removing ontology instances
- Searching instances that relations matches particular criteria

Current 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.

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. That gives opportunity to create interaction with other systems running in the network (such as IDS-Intrusion Detection System), that can take advantage from information stored in ontology and reconfigure if necessary.

4 CONCLUSIONS

In this paper we presented the results of FP7 ICT Project INTERSECTION.

Firstly, INTERSECTION Vulnerability Database (IVD) has been developed and described. 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 the security-resiliency framework. Moreover, PIVOT - ontology-logic based application has been developed and presented.

Both, IVD and PIVOT, can be used by end-users such as networks operators and telecoms to share and use knowledge about vulnerabilities as well as related threats and attacks affecting heterogeneous, complex and interconnected networks.

It is worth to mention that identified, classified and stored vulnerabilities have been provided by operators involved in the INTERSECTION Project (Polska Telefonia Cyfrowa, Telefonica, Telespazio). Therefore, IVD, IVO and PIVOT are based on real-life and actual information repositories.

ACKNOWLEDGEMENTS

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

Choraś M. (Ed.), Deliverable D.2.2 Identification and Classification of Vulnerabilities of Network Infrastructures, INTERSECTION Project, July, 2008.

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.

Shared Information/Data Model (SID), TeleManagement Forum, October 2002.

OWL Web Ontology Language Semantics and Abstract Syntax, June 2006, http://www.w3.org/TR/owl-features/.

SWRL: A Semantic Web Rule Language Combning OWL and RuleML, W3C Member Submission, http://www.w3.org/Submission/SWRL/.

Choraś M., Renk R., Flizikowski A., Hołubowicz W. (2008), "Ontology-based description of networks vulnerabilities" , Polish Journal of Environmental Studies, vol. 5c.

Choraś M., Kozik R., Flizikowski A., Renk R., Hołubowicz W. (2009), "Ontology-based Decision Support for Security Management in Heterogeneous Networks", In: Huang, D.-S. et al. (Eds.): Emerging Intelligent Computing Technology and Applications. With Aspects of Artificial Intelligence, LNAI 5755, Springer.