

THE INTERSECTION APPROACH TO VULNERABILITY HANDLING



Michał CHORAS*, Salvatore D'Antonio**, Rafal KOZIK*, Witold HOLUBOWICZ***
*ITTI Ltd., Poznan, Poland
email:michal.choras@itti.com.pl, rafal.kozik@itti.com.pl
**Consorzio Interuniversitario Nazionale per l'Informatica, Naples, Italy
email:saldanto@unina.it
***Adam Mickiewicz University, Poznan, Poland
email:holub@amu.edu.pl



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 heTeroogeneous, Resilient, SEcure, Complex, Tightly Inter-Operating Networks) - www.intersection-project.eu

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.

An ontology-based approach to vulnerability handling

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 reason about the objects in that domain and the relations between them.

Nowadays, we can observe an increasing complexity and heterogeneity of the communication networks and systems. Then the need arises to use high-level meta-description of relations in such heterogeneous networks. This need is particularly apparent in the context of Future Internet and Next Generation Networks development.

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.

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.

INTERSECTION Vulnerability Database

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.

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.

INTERSECTION Vulnerability Ontology

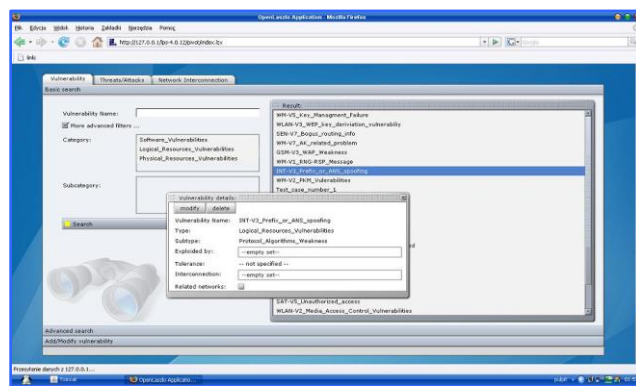
Networks assets should be defined and described. We decided to use Shared Information/Data (SID) Model in which networks assets and relations between them are defined. SID Model provides Physical Resource Business Entity Definitions. SID assets description is specified in UML and visualized using UML 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). Subclasses of Vulnerability class are:

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

ID	NAME	DISCOVERY DATE	DESCRIPTION	MITIGABLE TYPE
3	Key size in marginal	2005-06-25	The PKCS-#4 project, retrieved 04-bit keys by brute force in about 3 years using distributed Internet computing, which today (assuming Moore's law) could be done in less than a year.	GMN
47	Lack of Mutual authentication	2008-11-17	The bug flaw of the IEEE 802.11 security design is the lack of a authenticated 802 certificate. The only way to defend the client against rogue or replay attack is to provide a scheme for mutual authentication. No mutual authentication is provided. Two types of certificates are classified by IEEE 802.11 standard, one is for manufacturer certificates and the other is for SS certificates. There is no provision for 802 certificates. A manufacturer certificate identifies the manufacturer of an IEEE 802.11 device. It can be a self signed certificate or issued by a third party. A SS certificate identifies a particular SS and includes its MAC address in the subject field. Manufacturers typically create and sign SS certificates. In general the SS uses the manufacturer's certified public key to verify the SS certificate, and hence identify the device as genuine. This design assumes that the SS maintains the private key corresponding to its public key in a sealed container, preventing attacks from easily compromising it [2004].	WLAN
7	Media-Access control vulnerabilities	2005-06-18	The vulnerability has to do with the fair share of the transmission medium.	WLAN
41	Media-Access control vulnerabilities	2008-11-17	The vulnerability has to do with the fair share of the transmission medium. There are two different types of attacks that will help us to understand the idea of this kind of vulnerability. In the first attack, the physical carrier sense mechanism is attacked by sending a lot of short packets in rapid succession, and after that all nodes believe that the medium is already used by another node. All the other nodes are listening to the medium and are waiting for their turn to broadcast, but are unable to get their turn, as the attacker is transmitting continuously. In the second attack, the exploitation is completely different. The attacker sends packets very fast in contrast to the previous attack, but he uses longer length fields within the packet and the receiver gets a long transmitting packet, while the attacker is transmitting the attached nodes will not even try to use their carrier sense mechanism to send if the medium is busy. Attached nodes are starting the backoff and the transmission of the attacker ends, but unfortunately it will be a long time till then [2004].	WLAN



Project INTERSECTION Vulnerability Ontology Tool

PIVOT (Project INTERSECTION Vulnerability Ontology Tool) is the ontology-logic based manager tool. Our goal is 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 that the tool has a client-server architecture, which allows to share one ontology by multiple users (e.g. by network operators). PIVOT is designed to serve transactional operations over single ontology model. To accomplish this goal transactional SQL database is adopted to store ontology model and make significant performance improvements during I/O operations.

PIVOT provides the following basic functions:

- Searching vulnerabilities matching prompted criteria
- Adding, modifying ontology instances
- Removing ontology instances
- Searching instances matching specific criteria

Current version of PIVOT allows to establish two types of connections: the first type relies on RMI (Remote Method Invocation), while the second type uses HTTP.