Ontology Knowledge Bases of Security
Vulnerabilities, Attacks & Defenses

Patrick Kamongi, Mahadevan Gomathisankaran
patrickkamongi@my.unt.edu, mgomathi@unt.edu

Computer Science and Engineering
University of North Texas
Denton, TX 76203, USA

Work in Progress Abstract:

In this work, we present a rich generated Ontology Knowledge Base (OKB). This OKB is a result of the population tasks of three main ontologies (Vulnerabilities, Attacks and Defenses). Each one of the ontology is defined in terms of its classes and their related properties, and these properties in turn are used to express their roles in modeling security vulnerabilities, attacks and defenses. We implemented this OKB using Data feeds from multiple sources such as National Vulnerability Database [2] and open source Exploits Database [3]. Then we used Web Ontology Language (OWL) [4] modeling API to define our ontologies and instantiate them. The resulted OKB is to be used in our proposed framework for Vulnerability Assessment for Cloud Computing [1]. Within our proposed framework we can perform static analysis and dynamic testing of a given test system. As illustrated in Figure 1, each of the instantiated ontology is semantically linked to one other. For example our OKB of Vulnerabilities can be used to discover which attacks can exploit any given vulnerability from the OKB of attacks and vice-versa the OKB of attacks can look up which vulnerability is exploitable by one of its attack. Then the OKB of defenses can be used to mitigate attacks or countermeasure of the discovered vulnerabilities.

Figure 1 – Our Defined Ontology Knowledge Base

References

4. Web Ontology Language (OWL), http://www.w3.org/TR/owl-ref/