Ontologies for Modeling Enterprise Level Security Metrics

Anoop Singhal
Computer Security Division, NIST
Gaithersburg, Maryland, USA
psinghal@nist.gov

Duminda Wijesekera
Department of Computer Science
George Mason University
Fairfax, VA , USA
dwijesek@gmu.edu

EXTENDED ABSTRACT

Categories and Subject Descriptors
C.2.0 [**Computer-Communication Networks**]: General – *Security and protection (e.g., firewalls)*; K.6.5 [**Management of Computing and Information Systems**]: Security and Protection.

General Terms
Management, Measurement, Security.

Keywords
Security risk, attack graphs, security metrics.

1. Introduction

Currently, it is difficult to answer simple questions such as "are we more secure than yesterday" or "how should we invest our limited security budget." Decision makers in other areas of business and engineering often use metrics for determining whether a projected return on investment justifies its costs. Spending for new cyber-security measures is such an investment. Therefore, security metrics [1] that can quantify the overall risk in an enterprise system are essential in making sensible decisions in security management.

Information Security is a critical part for any enterprise. Often wrong decisions are made due to insufficient knowledge about the security domain, threats, possible countermeasures and the company's assets. There are several reasons for this. First, security terminology is not precisely defined, which leads to confusion among the security experts and the customers who should be served. Security ontologies are a viable solution for this problem because they allow a precise definition of the entities and their relationships to each other. Second, decisions about enterprise security are made by managers who do not fully understand the full depth of underlying IT infrastructure.

CSIIRW '10, April 21-23, Oak Ridge, Tennessee, USA

Their decisions are based on intuition rather than a thorough cost/benefit analysis. The main goal of our current research is to develop an ontology that has *knowledge* about which threats endanger which assets and which counter measures can reduce the probability of a damage. In our ontology each asset and each countermeasure can be annotated with various types of costs and benefits. This ontology can enable a quantitative risk analysis so that the manager of an enterprise can choose the appropriate safeguard mechanism to reduce the threats to their enterprise.

This paper is organized as follows. Section 2 presents a model for Enterprise Level Security. Section 3 discusses application of the ontology for collecting and querying data on security metrics and finally section 4 presents the conclusions.

2. Modeling Enterprise Level Security Metrics

It is important to have a data model for enterprise level security in terms of the entities and relationships among them. This data model can be used to measure the appropriate things to understand the effectiveness of current security mechanisms and the benefits that they provide. Modelers generally think about security in terms of threats, risks and losses. Good models provide a rationale for measurements and these data models can be updated and calibrated as new data becomes available.

2.1 The Design of an Ontology for Security Metrics

Ontology is a specification of a set of entities and their relationship. Consequently, an ontology can be created for any collection of related concepts. The main goal of our current research is to provide a security ontology framework to support IT security risk analysis. The ontology should know which threats endanger which assets and what countermeasures can lower the probability of the occurrence of an attack. A secondary goal was to develop an ontology in a framework such that the knowledge base is portable and easy to share. For this reason, we choose the Web Ontology Language (OWL). Readers that are interested in further details of OWL should refer to [2].

Figure 1 shows a graphical description of the ontology. The basic entities in the data model are:

1. **A threat** is described as a potential for violation of security when there is an event that can breach security and cause harm. An **attack** is an "assault on a system that violates the security policy of that system". An attack exploits vulnerabilities to realize a threat.
2. **Vulnerabilities** are characteristics of target assets that make them prone to attack and cause a certain loss or damage. For example, vulnerability can be a flaw or a weakness is a system design or implementation that can be exploited. Standard organizations such as Mitre

Corporation and First.org Inc. play an important role in modeling vulnerabilities. Mitre oversees Common Vulnerability Enumeration (CVE) and First.org oversees Common Vulnerability Scoring System (CVSS). Beyond this, there are several organizations that maintain vulnerability databases. Some examples are National Vulnerability Database (NVD) from NIST and DeepSight from Symantec Corp.

3. **Security Mechanisms** are designed to prevent the threats from happening or to mitigate their impact when they do. For example, a *firewall* is an example of a preventive control as it blocks bad traffic. An Intrusion Detection System (IDS) is an example of a detective control. It is important to have a measure of the effectiveness and efficiency for the countermeasures. Also accuracy is an important attribute of the countermeasure, which is defined as 1.0 minus the percentage of false alarms. The concept of *false positive* is often used to refer to the detection of an attack that turns out not to be one.
4. **Assets** are things that we plan to protect. An asset is a target of the threat and when the threat succeeds it results in a loss of value. Estimating the value of an asset is a difficult task. There is no formal methodology for assigning the value of an asset. Many assets in the network are primarily part of the IT infrastructure and they may not be involved in directly generating profit for the organization. For example, commodity servers and commercial software and networking products are part of the IT infrastructure. Many security products such as IDS and vulnerability scanners focus on these type of assets.
5. **Risk** is defined as an expectation of loss expressed as a probability that a particular threat will exploit a certain vulnerability that will result in a harmful result. The simplest way to quantify risk is to multiply the expected loss with the likelihood of a successful attack.

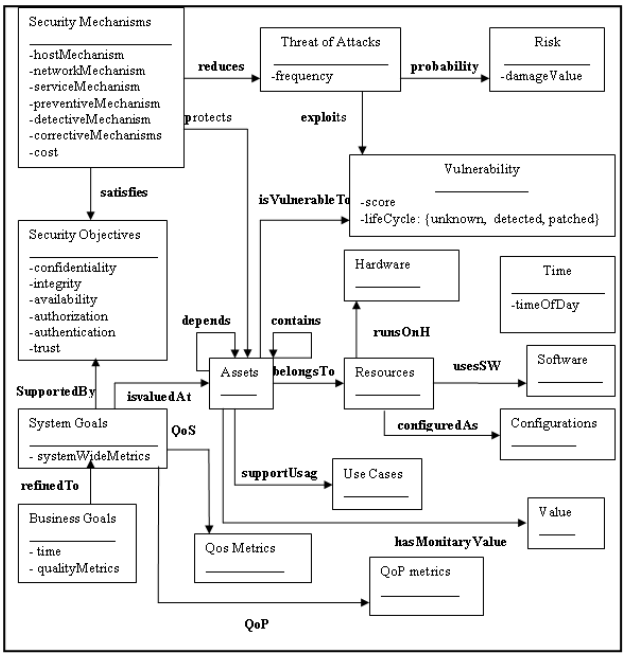

Figure 1: Entities and Relationships

Figure 2 gives a sample description of the Asset class in RDF.

```
1.  <rdf:Property rdf:ID=”value”>
2.     <rdfs:domain  rdf:resources=”Asset”/>
3.     <rdfs:range      rdf:resources=&xsd:integer/>
4.  </rdf:Property>
5.  <rdf:Property rdf:ID=”depends”>
6.     <rdfs:domain  rdf:resources=”Asset”/>
7.     <rdfs:range      rdf:resources=”Asset”/>
8.  </rdf:Property>
9.  <rdf:Property rdf:ID=”contains”>
10.    <rdfs:domain  rdf:resources=”Asset”/>
11.    <rdfs:range      rdf:resources=”Asset”/>
12. <rdf:Property rdf:ID=”isVulnerableTo”>
13.    <rdfs:domain  rdf:resources=”Asset”/>
14.    <rdfs:range      rdf:resources=”Vulnerability”/>
15. <rdf:Property rdf:ID=”belongsTo”>
16.    <rdfs:domain  rdf:resources=”Asset”/>
17.    <rdfs:range      rdf:resources=”Resource”/>
18. <rdf:Property rdf:ID=”monitaryValue”>
19.    <rdfs:domain  rdf:resources=”Assets”/>
20.    <rdfs:range      rdf:resources=”Value”/>
21. <rdf:Property rdf:ID=”supportUsage”>
22.    <rdfs:domain  rdf:resources=”Assets”/>
23.    <rdfs:range      rdf:resources=”Use Cases”/>
24. </rdf:Property>
```

Figure 2: Properties of the Asset Classes

3. Implementation and Application of the Security Metrics Ontology

We have implemented the ontology in OWL using Protégé [3] an Ontology Editor. Here we describe the application of the ontology for Enterprise level Security Metrics. The main application of the ontology is to collect data about security of the enterprise system and then query it to generate reports.

1) Collecting Data for Security Metrics
The entities defined in figure 1 can be translated into a set of database tables that can be used to collect information about an enterprise over a period of time and then generate reports and graphs about the performance and security of the enterprise.

2) Example Queries for Security Metrics

a) Find all Assets with value > 100K that have vulnerabilities that are published but not patched.
b) Generate a report that compares the number of vulnerabilities that were discovered but not yet patched, group by each month for the year 2008.
c) Which vulnerabilities are exploited by a given threat and which security mechanisms can be used to mitigate those vulnerabilities. How much do these security mechanisms cost? This query can help in doing a cost benefit analysis.
d) Suppose a vulnerability is discovered in a certain version of a shared library. Give me all products that use this shared library and are affected by it.

4. Conclusions

Defining an ontology is considered a main task within any scientific community. Our review of papers in the area of "Ontology for Information Security" [4], [5], [6], [7] indicated that the work is in early stages and there is a need to make more progress in this area. Increasingly, companies require accurate security concepts and plans to protects their assets. This demands an in-depth knowledge of existing threats, the company's assets and possible countermeasures. In this paper, we have developed an ontology for "Modeling Enterprise Level Security " using RDF and OWL. Knowledge of threats and corresponding countermeasures is integrated into this ontology framework.

The ontology guarantees a shared and accurate terminology and using OWL to represent it makes it portable. A prototype implementation of this ontology was used to generate reports about enterprise level security and do cost benefit analysis of security mechanisms.

5. References

1. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Addison Wesley, 2007.
2. W3C (2004) OWL Web Ontology Language Overview. http://www.w3.org/TR/owl-features
3. "The protégé ontology editor and knowledge acquisition system", http://protege.stanford.edy/ 2005.
4. Kim, J. Luo and M. Kang, "Security Ontology for Annotating Resources, 4th International Conference on Ontologies, Databases and Applications 2005, Cyprus.
5. G. Denker, Kagal L., and Finnin T., "Security in the Semantic Web using OWL, Information Security Technical Report, 2005, 10(1): pp. 51-58.
6. G. Dobson and P. Sawyer, "Revisiting Ontology-Based Requirements Engineering in the Age of Semantic Web", Workshop on Dependable Requirements Engineering of Computerized Systems, Institute of Energy Technology, Halden 2006.
7. J. Undercoffer, A. Joshi, and J. Pinkston, Modeling Computer Attacks: An Ontology for Intrusion Detection in the Sixth International Symposium on Recent Advances in Intrusion Detection, 2003.

Columns on Last Page Should Be Made As Close As Possible to Equal Length