Towards a Mathematical Model for Autonomously Organizing Security Metric Ontologies

Gregory Vert  
College of Security and Intelligence  
Embry Riddle Aeronautical University  
vertg@erau.edu

Bryce Barrette  
Global Security and Intelligence Studies  
Embry Riddle Aeronautical University  
Barretb4@erau.edu

Bilal Gonen  
Assistant Professor of Computer Science  
University of West Florida  
bilalgonen@gmail.com

Abstract:

Security metrics can be contextually related to the operation of the system and provide a static measure of system security. Some are better at determining the system security. However, their values can change dynamically to threat. Thus they can be grouped into ontologies measuring system health and security under threat conditions. The problem with current approaches is that they are static and that it does not consider the fact that metrics can also occur in multiple ontological classes. In this paper we develop and propose a model and mathematical grounds for ontologies that can dynamically reorganize based on the mathematical properties of the model. We initially develop a set of metrics that can then be incorporated into the ontological model that can autonomously reorganize into super and superior ontologies when threat is present. We identify sample of metrics to demonstrate the model on and evaluate the relations among metrics to develop the model. This work presents the initial relational model for autonomous recombination after developing the initial set of metrics and mapping them to ontological classes. This work is initial and conceptual with further work to be done in the future to empirically validate the model.

Keywords: Dynamic Organizing Ontologies, Security Metrics

I. INTRODUCTION

Computers are utilized in all major industries. Their value to these industries is incalculable and incredibly necessary to the function and continued profit of every industry that uses them. However, in return, cyber intrusion actively target these very computers and seek to defraud them of information or worse, disable their functions. Continued security improvements and infrastructure changes are necessary to maintain safety against these attacks. However, with numerous black markets for purchasing security exploit tools and hacking software’s readily available, it is a constant effort to stay ahead of cyber-attack developments. These attacks continue to grow in strength and become more encompassing of network security [1]. This proves especially true in areas such as cloud computing. As modern industry can choose to move their infrastructures to offsite servers, there exist very few frameworks for security. As this is the case, very different security frameworks and standards need to be developed than what is standard today [2].

The methods for improving this security must be taken with several factors in mind. Increasing security without proper attention to other factors involved with the network may create network vulnerabilities. To obtain proper and complete security, a balance must be maintained between security improvements and functionality of the network system. This analysis must be carried over to cover multiple information systems and the configurations they may take. This is critical for improving systems that are vastly interconnected [3]. For industry networks that carry very large integrated systems, this balance is very necessary to maintain. Even if a system can operate very efficiently and conduct operations quickly, without proper security protecting it, a cyberattack event may bring the company down. This mutual exclusivity of both factors leading to a successful network emphasizes the importance of this balance. Protecting functionality while maintaining security is paramount.

The issue is the limitations of current security metric coverage and scope limit their contribution to current security needs. Security metrics are singular in their focus, do not interact and are limited in their communication to security personnel. Additionally, no known framework exists for combining different metrics together or determine relationships from these individual metrics. This causes the current metrics that exist to provide incomplete and comprehensive security monitoring and solutions. The framework of this paper purposes solutions to expand their coverage and usefulness when addressing cyber security.

II. BACKGROUND

One way a security manager can interpret events about a system is through metrics. Security metrics are used by today’s professionals for determining the state of system security. Simply, metrics are a standard of measurement used to measure security factors within a network. [4]. As such, these metrics offer indicators for security management. By analyzing metrics, one can
find holes in the current systems, areas to improve, etc. This enables the incorporation of environmental factors into the creation of security metrics [5].

Research groups have attempted to develop security metrics over the years as they are an essential tool for system security maintenance and performance. However, the issue with current security metric systems is the static nature of these metrics. These metrics need to calculated and only accounts for a single indicator. While these are helpful for analyzing events, they are less helpful than they could be. Metrics should be taken and regrouped based on applicability to threat events in a system, creating much more descriptive and helpful metrics [6]. Ideally grouping would be autonomous and adaptive.

To enhance these metrics, adaptive methodologies can be applied to relevant security methods to improve their effectiveness. By adding adaptive methods, a much more tailored metric is produced for the security manager to interpret for their network security. Additionally, parameters can be fed into these security metrics to create a much more effective metric. The goal of adaptive metrics is to offer more effective indicators of system security that what is typical today. Such metrics should be developed and designed around multiple metrics and be based on a model that can be dynamically organized.

In addition, one issue that necessitates the use of adaptive security metrics is evaluating qualitative security methods to a quantitative measurable scale. This quantification is necessary to provide better understanding of complex phenomena and to enable informed decision making [7]. This enables security managers to be able to compare previous events in a uniform manner and easily compare with numerical readouts for their securities. In return, the manager can easily determine whether there is a need to decrease or increase security measures and in which areas to do so. Metrics of this quality can be used to assess network strength, find critical infrastructures of the network and suggest further coverage of future vulnerability based on past available historical data [8].

While there are defined metric systems, the goal of adaptive metrics is to create system that autonomously tailors itself to an individual system. [9]. To achieve this, there is a need to create metrics that are adaptable. To achieve this the following needs to be employed:

- Use policy to define security goals and properties
- Determine which objects within a security framework need to be protected
- Create methodologies that will collect and interpret data
- Develop a model for adaptive reorganization of metrics into groups of ontologies that can be utilized to measure system security under threat
- Develop framework for taking actions based on the results of the data.

The goal of this research is to define metrics that can be fit into ontologies of metrics that have mathematical properties and allow them to adaptively reorganize based on the types of threat present in a system.

The field is lacking autonomously defined models for security analysis [10]. These metrics will be a framework for implementation into the security framework. Additionally, the ontological model developed by this research enables easy applications to other areas of security in industry. In our initial research, we are developing the mathematics and the ontologies for creating relevant adaptive security metrics. This is referred as an adaptive security metric method (ASOMO).

The particular mathematics used for this work will be fuzzy sets. Fuzzy set theory in the developing model will allow metrics to be related to each other and thus placed in sets based on similarity. The fuzzy sets allow typical quantitative measures regarding security to be quantified in a meaningful way [12]. As an “underperforming” antivirus is a vague designation to compute, this makes analysis more difficult. However, when “underperforming” becomes a “.35” rating, mathematics can now be performed on metrics that otherwise could not.

Finally, the developing model will be an architecture or theory in practice. As the model’s theory is developing based on this initial work, the metric data will be utilized to test if the model works mathematically. The rest of the paper presents an initial development of security metrics ASOMO model that can then be mapped into autonomously self-organizing ontologies of security metrics. The mathematical basis for reorganization is defined. This is initial and ongoing work. The next sections will detail an initial determination and classification of security metrics, organization into ontological classes, and evaluation of the relations among metrics. Finally it will present the initial mathematical model for self-organizing ontologies as threat sweeps through a system.
III. APPROACH
A. Class designations and ontological mapping

The goal of ontological class designations is to designate a framework in which metrics could exist for a particular threat. These metrics can apply to a particular scenario in which a security manager will select a class of metrics to meet his security needs and match a security environment.

In order to relate the metrics to their particular ontological classes, we are examining how to utilize fuzzy set theory to determine similarity and membership. The derived values are approximated values assigned to particular metrics and score on a system relating to their presence within a security state set. This value could be designated as a 1, pertaining an complete membership in in ontological set class. Otherwise, a 0 is a designation of having no relation to a set. By relating the highest scoring metrics within a particular system, an ontological grouping of security metrics can be created using this method.

The first phase of the model was to determine that classes of security metrics that would then be mapped onto the ontological model. Our initial ontological classification of metrics is the following:

(i) User End- This Ontology requires direct input from the user or workstation within a network. These metrics are usually intended from security manager influence.

(ii) Server End- These metrics are directly influenced by company security policy. These metrics can also exist entirely internally as well, affecting nothing else but the company network.

(iii) Physical- These metrics relate to physical, natural places or objects. This can also apply to real-life incorporeal concepts like temporal events or security atmosphere after terrorist attacks.

(iv) Company Patch Risk- This metric covers the danger of a company-wide patch release. This is the amount of vulnerabilities to an entire network when a new patch is released.

(v) Physical Security- These are the actual physical assets a company may own to offer protection to their employees and/or networking equipment.

(vi) Reliability- The expected time duration the system is operating before it fails in delivering its service.

(vii) Criticality- The importance of particular computers on a network. Derived from location of the computer, service and applications running, role of the computer and asset value of the computer.

(viii) Temporal- Events pertaining to time based events in the present, past and future. Events more current may be more relevant or vice versa

In order to determine degrees of similarity between the above ontological classes, we developed for the model fuzzy linguistic variables as shown in figure 1. These are initial proposed values equally dividing the range of 0,1 to make a statement of the models evaluation of degrees of similarities among ontological metric classes.

\[
f(\text{similarity}) = \begin{cases} 
1 & \text{most similar (ms)} \\
0 & \text{not similar (ns)} \\
.5 & \text{somewhat similar (sws)} \\
.25 & \text{very unsimilar (vu)} \\
.75 & \text{very similar (vs)} 
\end{cases}
\]

Figure 1. Fuzzy Set Linguistics

For example, the metric Company Patch Risk resembles a 1, resembling a completely similar to the ontology “Physical”. This metric would then be assigned to the applicable ontology.

Table 2 represents the ontology similarity matrix. This will be used to determine super ontologies. This table takes two ontologies and, by using fuzzy set linguistics, their degree of relationship can be determined. The higher degree of relationship value found in the read outs of the ontology. The higher the degree of relationship, the stronger the two ontologies can be related. A high enough degree of relationship will designate them a super ontology and will be able to apply both to a security system equally.

<table>
<thead>
<tr>
<th></th>
<th>Company Patch Risk</th>
<th>Physical security</th>
<th>Reliability</th>
<th>Criticality</th>
<th>Temporal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sever End</td>
<td>vu</td>
<td>vu</td>
<td>sws</td>
<td>vs</td>
<td>vu</td>
</tr>
<tr>
<td>User End</td>
<td>vs</td>
<td>vu</td>
<td>sws</td>
<td>vs</td>
<td>vs</td>
</tr>
<tr>
<td>Physical</td>
<td>ms</td>
<td>vu</td>
<td>sws</td>
<td>vs</td>
<td>ns</td>
</tr>
</tbody>
</table>

TABLE 1. Ontological grouping by similarity
By using the linguistic variables, an autonomous update process can be put in place to dynamically calculate similarity. These groupings can also determine logical relationships between two metrics within an ontology.

Two high scoring metrics can perform in a similar fashion within the same ontology. For example as $\%$ Patch Risk $R \uparrow \%$ Vulnerability between Patch. However, the Inverse is also proven to be true. A metric scoring high and a metric scoring low within an ontology will have an inverse relationship; i.e. $\%$ Application Patch Risk $R \downarrow$ Safety.

Additionally, by looking at relationships among individual metrics, we can look at combined relationships of metrics within each ontology. If similar reactions to the initial mounted attack occur, this can show each metric within either ontology behave in a similar fashion. When enough of these relationships occur, two ontologies can be shown to be extremely related in security coverage. When this occurs a “super ontology” can be discovered.

The most unique feature of these “super ontology” is the adaptive nature in which they appear with the appropriate adaptive metrics. As such, these are dynamically created from any particular attack. The model for creation of super ontologies will be presented in subsequent sections of his paper.

These will offer large framework metric scenarios that future security work can select from for security solutions.

Autonomous nature to create these systems is also attempted to be proven within this research. Three criteria must be proven to ensure autonomy can be determined. Temporality is determined if two metrics increase following a mounted attack. This proves related behavior and increase a relationship between two ontology. Ontological relationships that increase in tandem can then show entire ontological relationship increases. Finally, correlation following an attack can be determined from the resulting increase ration from the metrics that make them up. Enough of this occurring can place them into “super ontologies following a threshold being reached. When all three of these conditions occur and a system measures it Table 3 represents the relationship between the metrics within the two ontologies $O_1 / O_2$ and how they interact with each other.

From our research, every metric included within these ontologies behave in a similar manner. The metrics identified as having more interactions within the security model will become the most important metrics per the security needs of the security manager. Adaptive features are realized by how the interactions change with different attacks, different metrics will behave between the ontologies; this will emphasize the importance of different metrics with each attack.

### B. Ontological Mathematics

The next premise in the model is that metrics dynamically associate and change to ontological groups based on the contextual threat they are facing. As an example the following metric relation could exist in multiple ontology's or across ontological classes:

$$\text{Patch}\{O_1\} = \% R \uparrow \%$$

which states that as the decrease in patch level (pl) occurs there is an increase in risk (r) and that this relation could be expressed in fuzzy set theory as the membership function $\text{Patch}\{,\}$. Quantification of these relations and the rules of the relation are the subject of ongoing work with the ASOMO model.

Based on the degree that these Ontological groupings are related through the similarity matrix, this can help determine how related ontologies are to one another. By determining which ontologies fit best with one another, frameworks can be determined for a best security model. Special autocorrelation is used in this case to show the strength of the relationships. The higher the number that is shown to participate in the relationship, the more correlated the two ontological systems become. Two highly related ontological classes will have metrics respond and thus correlate to a given threat scope or active threat.

In Table 3, some of the relationships between ontologies ($O_1$ and $O_2$) and metrics developed as part of this research are demonstrated. Our research shows there are logical arguments that arise from an attack as it affects each metric. For example, consider the metric patch risk (Pr), the introduction of new vulnerabilities when introducing a new patch, has the following interactions; there is an increase in implied patch risk (IPR). Data theft (DT) increases, the risk of an attack occurring with the purpose of bypassing security and stealing data. Correctness (Corr) decreases, the state of the system away from being “fully correct”. Reliability

<table>
<thead>
<tr>
<th></th>
<th>User End</th>
<th>Server End</th>
<th>Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server End</td>
<td>ns</td>
<td>ms</td>
<td>sws</td>
</tr>
<tr>
<td>Physical</td>
<td>sws</td>
<td>sws</td>
<td>ms</td>
</tr>
<tr>
<td>User End</td>
<td>ms</td>
<td>ms</td>
<td>vs</td>
</tr>
</tbody>
</table>

Table 2. Similarity Matrix
(Rel) decreases, the time in which a failed system is restored. Regularity (Reg) decreases, a state of strictly enforced security. Finally, Security Score (SS) decreases, value of the security of a network. The metric relations to other metrics are shown with up arrows denoting an increase and down arrows denoting a decrease. It is possible from our research to have the same metrics belong in multiple ontologies which leads to the next section were a model of combining metrics in super ontologies is presented. Such recombination $fn()$ - is a function considering of $O_1$ to $O_2$

$A$ - is a threat vector and $fn()$ returns a degree of relation utilized in the process of dynamic reorganization of ontology's composed of metrics.

C. Autonomous Ontological Mapping

Having defined a set of metrics that are candidates

<table>
<thead>
<tr>
<th>O_1 User End</th>
<th>O_2 Server End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patch Risk</td>
<td>Data theft</td>
</tr>
<tr>
<td>Availability</td>
<td>Data Loss</td>
</tr>
<tr>
<td>Reliability</td>
<td>Privacy</td>
</tr>
<tr>
<td>Correctness</td>
<td>Workstations (SBI)</td>
</tr>
<tr>
<td>Implied Patch Risk</td>
<td>Systems (AC)</td>
</tr>
<tr>
<td>Timer</td>
<td>Remote Endpoint Manageability</td>
</tr>
<tr>
<td>Criticality</td>
<td>Data Integrity</td>
</tr>
<tr>
<td>Security Score</td>
<td>Logging Coverage</td>
</tr>
<tr>
<td>Regularity</td>
<td>Vulnerabilities per Host</td>
</tr>
<tr>
<td>Vulnerability scanner coverage</td>
<td>Auditing and Log Files</td>
</tr>
</tbody>
</table>

Table 3 Metric Interactions Among Metrics and Ontologies

relation is stated in the following equation and the basis for combining ontologies of metrics into super and superior ontologies.

The relationship to threat in such a dynamically organizing system can be stated as the following:

$$f_n(O_1, O_2, A) = \{0, \ldots, 1\}$$

where:

- spatial attribute correlations
- temporal attribute correlations
- conceptual ontological correlations

In spatial correlations there is a relation such as that found over a network, where the ontological metrics are mapped over a network and have spatial adjacency as
malware may pass through the network and fall under the domain of a spatially correlated AOMO's. This scenario can occur as an attack sweeps through a network, penetrating deeper into the core of the system. The concept is modelled as shown in Figure 2.

![Figure 2. Spatial AOSMO modeling](image)

where:
- $O_x$ - are model adjacent ontologies
- $\uparrow$ - model metrics that are increasing as a result of threat as it sweep through lines - model a network topology

In the above figure, threat orginates at the right in the domain of $O_1$ and sweeps across the network causing other $O_2$ etc to respond with heightened metrics.

The mathematical relationship defined in the model is defined as:

$$O_1 \rightarrow O_2 \rightarrow O_3$$

Figure 3. Changes in one ontology imply changes in other ontologies.

stating that increases in metric activity or lack of, implies spatially adjacent AOSMO changes over time as the threat progresses.

Temporal attribute correlation does not have spatial adjacency but rather temporal adjacency. For the purposes of this model, the mathematical relationship is defined as the following:

$$\uparrow O_{10} \rightarrow \uparrow O_{20}$$

Figure 4. Temporal relation among ontologies

where:
- $O_x$ - are temporally related ontologies
- $\uparrow$ - indicates increases in metrics in ontology

This relation implies that at time $T_0$ an increase one ontologies metrics results in another ontology have a direct relation and increase.

Finally, the conceptual ontological correlation does not look at time or spatial adjacency per se it only looks at the number of metrics in an ontology that increases in response to a specific threat. The relation is defined as the following:

![Figure 5. Ontological attribute coorelation](image)

where:
- $O_x$ - are different ontology's over a given domain responding to a category of threat
- $\uparrow$ - model metrics that are increasing as a result of a specific threat
- $\rightarrow$ - indicates metrics that have not changed for metrics $a_x$ and $b_x$

Work is looking at how to fuzzify the metrics into fuzzy linguistic variables in set theory such as the following example.

Metric$_x = \{\text{very good}, \text{good}, \text{ok}, \text{not ok}\}$

Finally the AOSMO model defines the concept of a superior ontology

Empirical work is planned for the future, but intially the model defines a superior ontology to be given as:

$$S_{O_1} \cap S_{O_2} > 50\%$$

Figure 6. Criteria for creation of a 'super' ontology

where:
- $S_{O_x}$ is the set of metrics in onotolgy $x$

A super ontology is defined in the model as

$$S_{O_1} \cap S_{O_2} > 90\%$$

Figure 7. Criteria for creation of a super ontology

where:
- $S_{O_x}$ is the set of metrics in onotolgy $x$

The criteria for a super and superior ontology provide the basis for recombination of ontologies in the AOSMO model. In addition, the numeric criterion can be autonomously adjusted programatically and
implemented in software relatively easily. The relation of super and superior can be stated as the following

\[ \uparrow O_1 \cap \uparrow O_2 \rightarrow O^{Super^\prime} O^{Superior} \]

*Figure 8. General correlation rule*

Simply put, this relation states that increases in metric levels for different ontologies 'can' imply the result of a reorganized 'super' or 'superior' based on the relations previously presented.

Similarities by Fuzzy (move to attributes)
Working on Statistical measures of significant similarity

IV. CONCLUSIONS

This initial work provides the structural model and framework for a system of dynamically and autonomously self-organizing ontology's derived from initial work with defining a set of metrics to operate over. This model used a semi-autonomous approach to correlate relationships based on input metrics. The fuzzy sets allowed for gradient relationships to be formed and evaluated.

Future work can continue to evaluate the definitions and methodology for creating and evaluating the metrics and ontologies used within the model. The proposed ontologies are hypothetical and may or may not be used in an implemented model within a security environment. Therefore, future research can choose which metrics are to be evaluated and organized by the model, and which ontologies can be produced by the data.

The work is initially modeling of a system that could be implemented programmatically. Future work needs to empirically evaluate and validate the models concepts and relations. It also needs to examine the methods of traditional correlation as it might relate to the role fuzzy linguistic variables in the model.
REFERENCES:


Oct. 2014
doi: 10.1109/MILCOM.2014.53

