OPEN PLATFORM FOR ATTACK AND COUNTERMEASURE ANALYSIS ON SYSTEM SECURITY

by

Özgün Bal

B.S., Electrical and Electronics Engineering, Boğaziçi University, 2014

Submitted to the Institute for Graduate Studies in
Science and Engineering in partial fulfillment of
the requirements for the degree of
Master of Science

Graduate Program in Electrical and Electronics Engineering
Boğaziçi University
2018

ACKNOWLEDGEMENTS

I would like to thank my parents Berrin and Zeynel for their endless support and encouragement in all decisions I made. I am lucky to have such family that raised me as independent and confident person.

I express my gratitude to Professor Emin Anarım, my supervisor, for his support in this study. Furthermore, his guidance was important for me through the graduate program. I also would like to thank my other advisor Professor Mutlu Koca to his support in this research and thesis.

I would like to give a special thanks to Alev Ecevitoğlu for moral assistance in the long period of research and thesis writing.

This thesis is supported by the research of the Scientific and Technological Research Council of Turkey (TUBITAK) under the project number 117030.

ABSTRACT

OPEN PLATFORM FOR ATTACK AND COUNTERMEASURE ANALYSIS ON SYSTEM SECURITY

Attack detection and prevention is an essential subject in contemporary security practices. Like early detection of attacks, fast decision that includes optimum option is also an important issue. Selection of right prevention is a job of IT experts but they need well extracted data such as metrics, figures and tables. The whole process can be called a countermeasure selection. Countermeasure selection not only related to diminishing attacks' effects but also spending minimum money on that issue. That means investment upon countermeasure should be well spent. Return on response investment is a crucial aspect to satisfy company's needs. For this purpose, this work relies on RORI index to decide optimum countermeasure in the system under attack.

To be able to visualize attacks and countermeasures in the system, geometrical models are used. These helps to see affected area or volume under attack. Other than visibility, models provide calculation of attacks' or countermeasures' percentage in the system.

In this work, attacks against security vulnerabilities and countermeasures are investigated. Attacks and countermeasures are displayed in 3 dimensional volume model and n-sided polygonal model. In the application, these geometric visualization helps to analyze attacks and countermeasures in the context of system security. In addition, calculation of RORI index provides comparison between countermeasures in a numerical way.

ÖZET

SİSTEM GÜVENLİĞİNDE SALDIRI VE KARŞI ÖNLEM ANALİZİ İÇİN AÇIK PLATFORM

Günümüzdeki güvenlik uygulamalarında saldırı tespiti ve önlenmesi önemli bir konudur. Saldırıların erken tespit edilmesi kadar en uygun çözümün hızlı bir biçimde seçilmesi de önem kazanmaktadır. Doğru önlemin seçilmesi BT uzmanlarının işi olsa da iyi çıkarılmış sayısal, grafik ve tablo gibi verilere ihtiyaç duymaktadırlar. Bu işlemin toplamına karşı önlem seçilmesi denilmektedir. Karşı önlem seçimi saldırı etkilerini azaltmanın yanında en az miktarda para harcanmasını da dikkate alır. Bu da karşı önleme yapılan yatırımın doğru bir şekilde harcanmasını gerektirir. Yatırımın geri dönüşü(RORI) kurumların ihtiyaçları ile uyuşan önemli bir etkendir. Bu yüzden saldırı altındaki sistemlerde en uygun karşı önlemi seçebilmek adına, bu çalışma RORI indeksine güvenmektedir.

Sistemdeki saldırı ve karşı önlemleri görsel olarak sunabilmek için, geometrik modeller kullanılmaktadır. Bunlar saldırıdan etkilenen alan veya hacmin anlaşılmasını sağlar. Görsellik dışında da saldırı ve karşı önlemlerin sistemdeki yüzdelerinin hesaplanmasına yardımcı olur.

Bu çalışmada, sistemlerdeki güvenlik zafiyetlerini hedef alan atakları ve bunları engellemek için oluşturulan karşı koyma önlemleri incelenmiştir. Atak ve karşı önlemler hem 3 boyutlu uzayda hacim olarak, hem de 2 boyutta n-kenarı olan bir poligon şeklinde ifade edilen modellere dayanmaktadır. Yapılan uygulama sistemdeki atak ve karşı önlemleri geometrik olarak analiz etmeye yardımcı olmaktadır. Ek olarak, RORI indeksi bulunması ile karşı önlemler sayısal olarak karşılaştırılmaktadır.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS/ABBREVIATIONS

2D	Two Dimensional
3D	Three Dimensional
AIV	Annual Infrastructure Value
ALE	Annual Loss Expectancy
ARC	Annual Response Cost
ARO	Annual Rate of Occurrence
CF	Conversion Factor
COV	Coverage
DDoS	Distributed Denial of Service
EF	Effectiveness Factor
PCD	Potential Collateral Damage
RFIA	Response Financial Impact Analysis
RCU	Resource-Channel-User Account
RM	Risk Mitigation
ROIA	Response Operational Impact Analysis
RORI	Return On Response Investment
SLE	Single Loss Expectancy

1. INTRODUCTION

Starting with [1]'s definition of cybersecurity, it can be said that system security ensures availability, integrity, authentication, confidentiality and non-repudiation by preventing damage, protecting and restoring electronic communications including contained information in it. Attempts to break those attributes are considered attacks to the system. Finding solution after such attacks and protection scenarios from potential attacks are countermeasures in the context of security. One of the important issues about security systems is detecting attacks on the system and selecting countermeasures towards them. Attacks which may affect many units of the system may be encountered in the past or may be a new attack for the companies. Security experts at the companies should have countermeasure scenarios for possible threats. Other than specific countermeasure option, combination of countermeasure scenarios can also be applied to prevent attacks' effects as soon as possible. For example, unusual behavior of administrator account can be considered as an attack. Countermeasure scenario for such threat can be renewal of account's password and informing true owner of the account after that.

Many companies need a risk assessment on security problems and risk assessment still keeps popularity in security area. Every day, knowledge of attackers increase and technology evolves continuously. As a result of that companies should be more cautious and should plan their future carefully. That's why companies are investigated under certain attack scenarios to assess potential threats. Steps for the risk management are defined as framing, assessing, responding and monitoring [2]. Reports of these assessments are given to security experts. They can choose proper countermeasure manually but this doesn't sufficient for all the times. In small companies, experts can follow risk diversions and choose needed plan. However, in medium or big size companies, it's not viable to follow risk assessments and select relevant countermeasure towards them without automatic processes. Hence, dynamic countermeasure selection is important in terms of managing access control systems well and fast decisions about attack prevention [3].

Identity Access Management units try choosing best countermeasures to prevent known or unknown attacks. The decision can be made by the influence of minimum coverage of attack, maximum cost and the best return on response investment (RORI) index [4]. A countermeasure has a financial damage on companies so optimum countermeasure selection is an essential subject to keep the cost at optimum level. Such decision making processes need supportive evidences and useful methods. To achieve this, attacks and countermeasures in the system are expressed with certain models. At [5], countermeasures and related cost calculations are done with countermeasure graph model. Geometric models at [6] provides both attacks' and countermeasures' impact on the system objectively. Percentage of attack coverage can be observed with respect to chosen countermeasure. Addition to this, RORI index is calculated to satisfy minimum money spending condition. Best RORI option is represents right countermeasure scenario that involves compromise between desired attack coverage and upper limit of reaction cost.

It's important for companies to keep stable their security. So fast and right decisions should be made when there's an active attack to the system. Beside that, decision should be at the optimum level considering financial concerns of the company. To solve such problems, geometric models and RORI index are helpful. Even though, these methods are exist, it wouldn't be safe to assume that they fit every companies' needs. That's why it's good to provide tests in simulation environment to gain companies' trust. This work provides visual and metric data without too much technical details when company needs to investigate current security of the system. Eventually, comparison between countermeasure scenarios and selection of best countermeasure is the aim of the open platform.

2. LITERATURE SURVEY

In the context of system security, defining security events is initial step of understanding the system that are investigated. Security events are attacks, threats, responses or countermeasures at the system. Those events can also be considered as security metrics and they need to be expressed with certain models. Work in [6] separates visualization techniques of security metrics in to two. One is geometrical models and other is graphical models. Geometrical models consists polygons, rectangular and other type of prims. Major graphical models are chart and graphs. This work also compares complexities and data descriptions of models. At the end, examples of visualization models are given with supportive case studies.

There are two analysis method for countermeasure selection is introduced in [7]. One is response financial impact assessment (RFIA), other is response operational impact assessment (ROIA). Countermeasures named as mitigation actions that try to prevent threats. RFIA focuses economic concerns related to selection of mitigation actions. RORI index is used for ranking those actions. Mitigation action with higher RORI index is a better option to defend the system. ROIA makes its assessment using dependency model of nodes at the organization. Nodes at the generated dependency graph transmit impact to neighbor nodes so unpredicted parts of the system also affected by a mitigation action. That's why ROIA is combined with RFIA as an complimentary methodology. It makes sure result of RFIA doesn't conflict with the result of ROIA.

Work in [8] investigates information of the system security in terms of event data. Critical or non-critical systems, logical or physical systems are determined. Given events can be visualized with the help of geometrical models. Three dimensional event representation is used with the example data. Comparison of visualization models are discussed.

Attack graph model is used in both [9] and [10]. Probability calculations of graph nodes under attack is made. Response selection depends on countermeasure index which examines risk of the system before and after the countermeasure. Countermeasure with least side effect has a higher index. Effectiveness and damage scores are considered in index calculation. Economics of countermeasure selection is not primary goal. Another study that works with attack graphs is related network intrusion detection is mentioned in [11]. Focus of work is detection of Distributed Denial of Service (DDoS) attacks. Due to attack structure, it needs early stage actions, vulnerability detection, measurement and countermeasure selection in cloud virtual machines. Provided method is calculation of distance between attacked node and countermeasure point of selection.

Dynamic risk management response system is an another study that system security is mentioned in [12] with the context of attacks and countermeasures. This work also depends on attack graphs to express entry points of threats on the system. Threats are examined with the help of their likelihood of success. For evaluation of countermeasures, ROIA is used to determine operational impacts of countermeasures to the organization. Side effects of responses are considered when choosing one solution from available countermeasures list.

Countermeasure selection is a useful practice for access control system. In [13], security policies are defined with organization based access control model. It uses abstract entities which are roles, activities and views in the organizations. Countermeasure pool is designed with the use of those entities. Criteria for countermeasure selection is RORI index to choose optimum solution.

Different approach of deciding security investments is examined in [14]. This research's main focus is finding cost friendly investment options for the sake of organizations. Events of the system also includes recruitment processes and audits in addition to threats. There are four constraints to decide security investments. Those are security risks, compliance, productivity and cost. To be able to satisfy all of four constraints at certain level, utility function optimization technique is used. This approach works

with historical data of the system because it gives a solution by examining past relevant data which depends on case study of a company. Internal parameters decided with help of business interests. This work fits to check the system's security efficiency in regular periods. Dynamic selection of investment options is not in the scope.

3. RETURN ON RESPONSE INVESTMENT

The Return on Response Investment (RORI) is a model for expressing cost sensitivity of a response and it provides financial comparison between responses. It was first explained at [15] then RORI index makes easy to choose optimum investment option among others.

In the context of security, investment is defined as protection of the system from possible attacks. These protections may be chosen before any attacks exist or after the attacks occur. At [4], RORI index is proposed to be used for deciding protections at the system. In other words, RORI index is an indicator of how good that countermeasure is against attack or attacks at the system. RORI index can be calculated according to following equation:

$$RORI = \frac{(ALE \times RM) - ARC}{ARC + AIV} \tag{3.1}$$

where:

- ALE is Annual Loss Expectancy which is financial impact of the cumulative attacks on the system in a one year period. ALE is calculated with (3.2) as an product of Single Loss Expectancy (SLE) and Annual Rate of Occurrence (ARO). SLE means economic damage of the attack on the system when encountered only one time. ARO is estimated according to probability of observing the same attack in a year repeatedly. When ARO is 12, a specific attack is launched approximately every month.

$$ALE = SLE \times ARO \tag{3.2}$$

- RM is Risk Mitigation which is a ratio of attack prevention by countermeasures. At the condition of system under attack and no countermeasures, value of RM

is zero. Its value changes between 0-1. With the help of (3.3), RM is calculated as a product of Coverage (COV) and Effectiveness Factor (EF). COV represents percentage of protected parts of the system on the units under attack. COV calculation can differ according to chosen geometric model for the system. EF is a fixed value for chosen countermeasure.

$$RM = COV \times EF \tag{3.3}$$

- ARC is Annual Response Cost which is amount of money to be spent on chosen one countermeasure or combination of many countermeasures in one year. ARC is needed for implementation and maintenance of countermeasure and it's directly proportional to quantity and capacity of chosen countermeasures.
- AIV is Annual Infrastructure Value which is summation of yearly expenses such as equipment, personnel and services etc. AIV doesn't be affected by attacks and countermeasures. It is a fixed cost for the given system.

4. GEOMETRIC MODELS FOR SECURITY ATTACKS

4.1. 3D Attack Volume Model

Attack Volume Model defines the system as a 3 dimensional space in a context of security. That volume comprises channels, resources and user accounts which they are essential parameters of the system. These can be explained like following:

- Resource: It consists of physical and logical elements in the system. Physical elements can be server machine, printer, scanner etc. Logical ones are digital records like logs, database which are created by computers.
- Channel: This is interpreted as communication channel or bandwidth. The role is providing users to reach resources. Channels like IP, port number and bandwidth are defined by the companies at the installation of the system.
- User Account: It is a specific definition to provide connection and interaction of person with the system. An account represents rights and position of a person in the organization. Examples of accounts are administrator account and standard user account in the company's authorization mechanism.

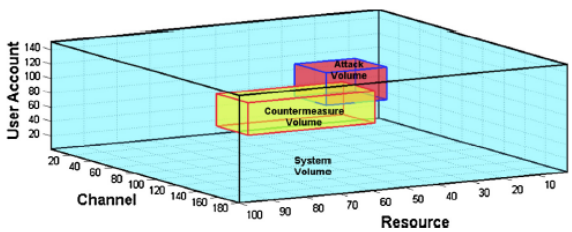


Figure 4.1. Attack Volume Model

Each of parameters defined above are dimensions of a system. A dimension has smaller units which constitute range of an axis at 3D volume. Because units may differ in terms of quantity and weight, the length of a unit in one dimension is different than others. An example system is represented at Table 4.1 . Every unit has own quantity, weighting factor and range in a dimension. Product of quantity and weighting factor

gives length of an unit. Summation of units' lengths provides a dimension of a system. Weight of each unit is decided by the CARVER methodology that explained at [4]. As a short summary, weighting factor of an unit is determined by six factors. Those are criticality, accessibility, recuperability, vulnerability, effect and recognizability. A score is given between 1 to 10 for each factors then summation of the scores is expressed as a weighting factor of an unit. At [4], chosen weights are in a range between 0 and 5 but weights in Table 4.1 are from 1 up to 10 which is average of CARVER scores.

Table 4.1. Example RCU information of a system

Dimension	Range	Description	Quantity	Weight	Distance
Resource	R1:R2	Server	2	7	1:14
	R3:R4	Power Supply	2	5	15:24
	R5:R6	PC	2	3	25:30
Channel	C1:C1	TCP	1	9	1:9
	C2:C3	IP	2	5	10:19
	C4:C5	Other	2	2	20:23
User Account	U1:U2	Super Admin	2	9	1:18
	U3:U4	Admin	2	8	19:34
	U5:U6	Guest	2	1	35:36

4.1.1. Volume Calculations at Attack Volume Model

Attack Volume Model consists quadrangular prims which expresses the system, attack and countermeasure volumes like explained at [16]. Attacks and countermeasures are in the system volume like Figure 4.1 displays. To be able to get numeric data related to the system, attacks and countermeasures, volume calculation of such quadrangular prisms is needed. Required input for the calculation is similar Table 4.1.

Following equation helps to calculate single axis of an prism:

$$L_{Dim_j}(S) = \sum_{i=1}^{n} q_i \times w_i \tag{4.1}$$

where Dim_j is one the dimensions of the system -resource, channel, user account- and L_{Dim_j} is the length of that dimension. n is the number of unit in that dimension. q_i is quantity and w_i is weighting factor of a unit.

Calculation of the system volume is provided by product of every dimensions' length like below:

$$SV(S) = \prod_{j=1}^{3} L_{Dim_j}(S) \tag{4.2}$$

similar calculation is also made for attacks and countermeasures. Following equations express their volume formula:

$$AV(S) = \prod_{j=1}^{3} L_{Dim_j}(A) \tag{4.3}$$

$$CV(S) = \prod_{j=1}^{3} L_{Dim_j}(C) \tag{4.4}$$

Most important benefit of the volume calculations is determining coverage of the attack volume by the chosen countermeasures' volume. Because this gives an indicator when choosing optimum countermeasure option amongst all possible scenarios. Attack coverage of an countermeasure is found as following:

$$Cov(C/A) = \frac{CV(C \bigcap A)}{AV(A)} \times 100 \tag{4.5}$$

For calculation of covered volume $CV(C \bigcap A)$, volume intersection is done. Also, attack and countermeasure volumes in the (4.5) are union of volumes if there are more than one. The system may under many attacks or more than one countermeasures are need to prevent threats.

4.2. N-sided Polygonal Model

This model that explained at [17] assumes systems in security domain are consists n dimensions. With using RCU information as a basis, there are 3 dimensions that constructs 3-sided polygonal i.e. triangular. The system, attacks and countermeasures are expressed as a triangular in a 2D space. If it's derived more information from the context of the system, more dimensions can be added to system additional to RCU.

An example representation is at Figure 4.2. 100 is boundary of the dimension which is the system's value by default. Any attack or countermeasures has a value between 0 and 100 for each dimension. Connection of the points on the dimensions creates an n-sided polygonal.

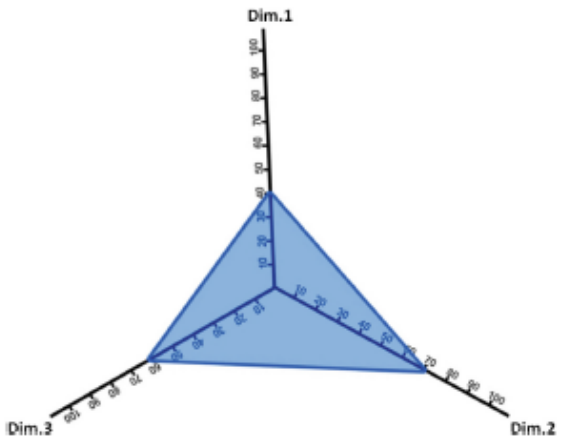


Figure 4.2. N-sided Polygonal Model (n=3)

4.2.1. Dimension, Perimeter and Area Calculations

N-sided polygonal model based on contribution of n dimensions. Those help to draw 2D geometric representation as the model suggests. Contribution of one dimension is calculated as following:

$$Co(Dim_j, E) = \frac{\sum_{k=1}^{m} q_k \times w_k}{\sum_{l=1}^{n} q_l \times w_l} \times 100 \tag{4.6}$$

where $Co(Dim_j, E)$ is the contribution of dimension j with respect to event E on the system. Event can be an attack, countermeasure or cumulative attacks and countermeasures. n is the number of total units on Dim_j at the system. m is the number affected units on Dim_j by an event. q is quantity of a unit and w is weighting factor given according to CARVER methodology.

Perimeter of the polygon is one of the indicators that model suggests. In most general form, formula of an irregular polygon is as following:

$$P = \sum_{i=1}^{n} L_i(E) \tag{4.7}$$

where L is the length of a side of the polygon with n sides.

Area of the polygon is an another indicator to choose optimum countermeasure option on the system according their values. To be able to the find area of an irregular polygon and all others, following formulation is used:

$$A = \frac{\sum_{i=1}^{n} Co(Dim_i, E) \times Co(Dim_{i+1}, E)}{2} \tag{4.8}$$

where dimension contributions are multiplied sequentially. On the last iteration, $Co(Dim_1, E)$ is used instead of $Co(Dim_{n+1}, E)$.

5. TOOL IMPLEMENTATION

In the light of RORI and geometrical models for system security, one should be able to decide attack prevention with minimum cost and maximum efficiency. In theory, it is possible and achievable to choose best countermeasure to cover attacked units at the system. However, many calculations and including more than one research topic can be confusing for decision making people at companies. That's why there's a need to abstract such technical details from end user. In this context, end users might be IT experts or even stake holders that decide which countermeasure investments would be done.

All reasons above lead to build a tool for selecting optimum countermeasure against attacks on the system. Aims of such tool are being easy-to-use, accessible from everywhere and creating proper simulation environment. Building as a web application that executes on a Internet browser provides accessibility goal. Every device that connects to Internet can access the content and use related to desired needs. Easy-to-use user experience can be achieved with abstraction of technical expertise in this topic. User should only needs the information about its system, attacks, countermeasures and costs of them. Then, given input is processed at tool's black box implementation. Final output will be numeric and graphical tips to choose best countermeasure scenario for ensuring both cost and coverage efficiency. Tool also provides good simulation environment to try and simulate methods in the literature in a real life problem easily. Dealing with countermeasure investments can cause a lot of negative financial impact if it's not done right. Hence, giving an opportunity to run simulations in safe environment is beneficial to decision makers at the organizations.

5.1. Data Models

Data Models in the implementation are system, attack and countermeasure. They are constructed as a class which can be part of object oriented design principle in software development [18]. Figure 5.1 shows what variables are needed as an input

and outputs of the system data model. RCU info of the system is similar to Table 4.1 and AIV is defined as a parameter of (3.1). Infrastructure value is an installation cost of the system. Those are inputs of the model. Outputs are calculation volume of the system in $units^3$, Conversion Factor(CF) and coordinates of the system for drawing as quadrangular prism in 3D. CF is a cost of 1 $units^3$ so i.e. it's find by dividing infrastructure value by system volume.

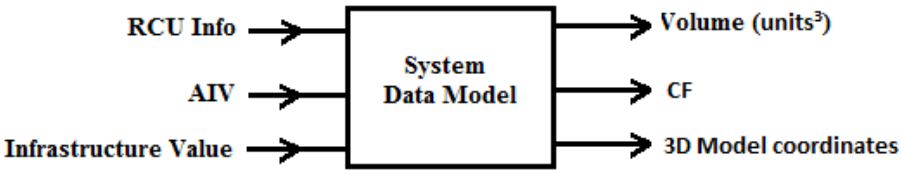


Figure 5.1. System Data Model

Attack data model takes instance of the system data model, ARO and attack string as inputs. ARO is defined at (3.2). Attack string is an identifier of which units of the system are under attack. An example attack string has a form like *R(1-3)C(2)U(4-6)*. Meaning of the string is interpreted by Message Engine. Result of the interpretation tells that first three units of the resource dimension, second unit of the channel dimension and four to sixth units of the user account dimension are under attack. Number of the attack strings can be more than one when multiple attacks occurred. Outputs of the model are also listed at Figure 5.2. ALE is defined at both (3.1) and (3.2). RCU information is an interpretation of the attack string by Message Engine. Dimension contributions are needed values for N-Sided Polygonal Model for both draw and calculations. Coordinates are for drawing the attack in the 3D Attack Volume Model.

Besides EF, inputs of the countermeasure data model are similar to attack data model as displayed at Figure 5.3. Countermeasure strings have a same form as attack strings. Only difference is countermeasure strings refer to protected units in the system. Again similar to attack data model, countermeasure strings may also be more than one when chosen countermeasure scenarios including many solutions. Each coun-

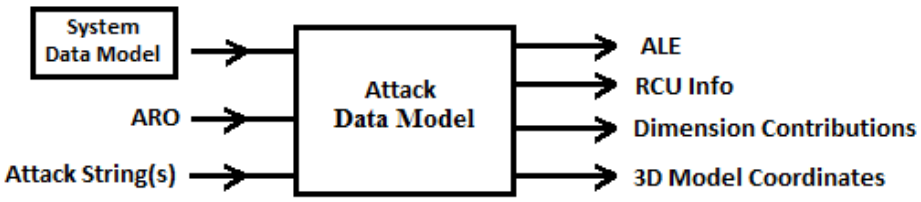


Figure 5.2. Attack Data Model

termeasure has own EF value like defined at (3.3). When multiple countermeasures exist, chosen effectiveness factor is the lowest one amongst others for the instance of a countermeasure data model. Dimensions contributions and coordinates are provided for geometric models as stated in attack data model. RM and ARC is defined at (3.1). COV and also RM is mentioned at (3.3). Potential Collateral Damage(PCD) is side effect of the countermeasure on the system where units are not under attack but covered with countermeasure scenario.

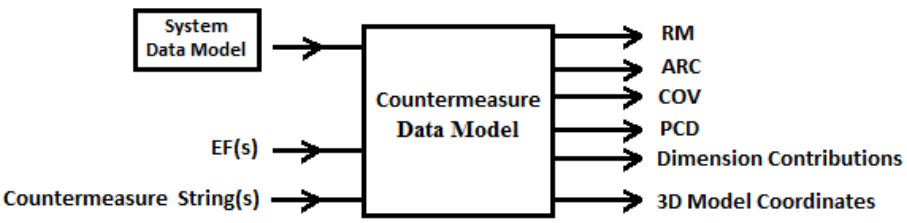


Figure 5.3. Countermeasure Data Model

5.2. Engines

Engines are modules that make necessary calculations and acquire desired information from input data. They act as a middle men between inputs and outputs.

Attack and countermeasure strings are mentioned in section 5.1. To be able to get RCU information of such event, string should be parsed and a module should get related unit information at the system. This module is a Message Engine that is state

at Figure 5.4. Event (attack or countermeasure) string has form like following:

$$Dim_i(start_i - end_i)Dim_{i+1}(start_{i+1} - end_{i+1})...$$

where Dim_i represent *i-th* dimension's capital initial. $start_i$ and end_i are number of units where the event affects the system. In this tool's context, dimension initials are R, C and U which represent resource, channel and user account. Message Engine maps event strings to RCU information of an event by using RCU information of the system as a lookup table.

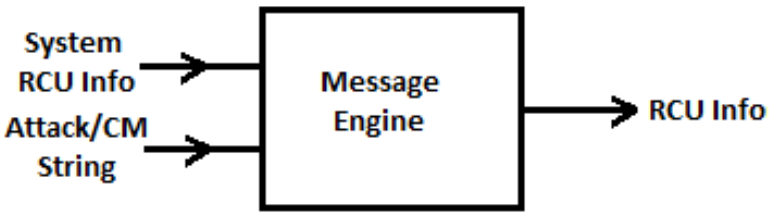


Figure 5.4. Message Engine

Attack Volume Engine calculates volume of the system or an event. Necessary input of the engine is RCU information. AV Engine also computes union and intersection of volumes. When there are multiple countermeasures or attacks, union of such volumes should be found to observe effect of the event on the system. Intersection is needed to find coverage of a countermeasure over an attack. Intersection of them demonstrate protected units from attack. As Figure 5.5 states, input of AV Engine is single or multiple RCU information. Outputs are calculated volume in $units^3$ and calculated RCU information of union or intersection.

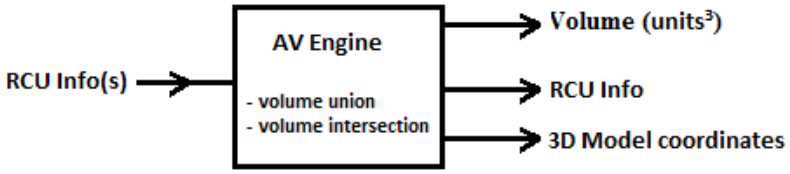


Figure 5.5. Attack Volume Engine

Polygon Engine is similar to Attack Volume Engine in terms of input and internal calculations. This engine also makes union and intersection operations but for dimension contributions and area of the polygons. Perimeter of a polygon is computed with (4.7) and area is with (4.8).

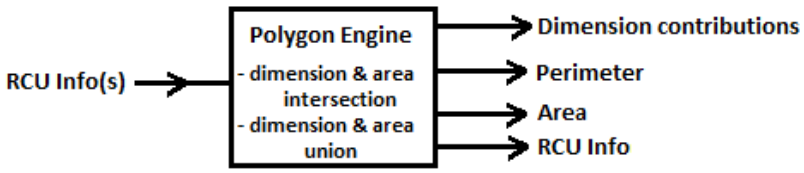


Figure 5.6. Polygon Engine

Last engine of the implementation is RORI Engine that calculates RORI index with the instances of data models. Inputs are derived instances from system, attack and countermeasure data models. They contain the related information that is what their model provide. Output can be more than one RORI indexes when countermeasure data model has several defense scenario on the system. Each combination of the given scenarios creates different RORI index.

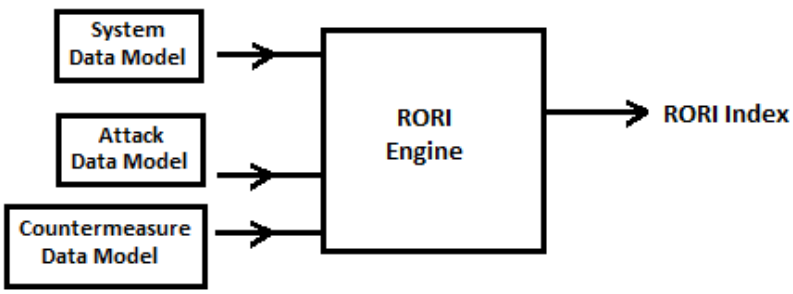


Figure 5.7. RORI Engine

5.3. Simulations

Data models and engines provide necessary instruments to create and run simulations. The tool supports two geometric models for defining the system, attacks and countermeasures so two simulation options exist. One is simulation of 3D Attack Volume Model at Figure 5.8. Other is simulation of N-sided Polygonal Model at Figure

5.9. Both have same inputs which are inputs of each data models separately. Outputs differ because their engine that is specific to geometric model is different. This variation can be observed by looking Figure 5.5 and Figure 5.6. Both has drawing data for the graphical user interface (GUI). However, drawing data of each model has a different structure. And, only Attack Volume Model has outcome of RORI indexes. They both provide coverage(COV), potential collateral damage(PCD) and residual risk(RR) as numeric identifiers of a countermeasure. PCD and RR calculations are done by following:

$$RR = 100 - COV \tag{5.1}$$

$$PCD = \frac{CV(S) - Cov(C/A)}{CV(S)} \times 100 \tag{5.2}$$

where COV is defined at (3.3). $CV(S)$ is mentioned at (4.4) and $Cov(C/A)$ is at (4.5).

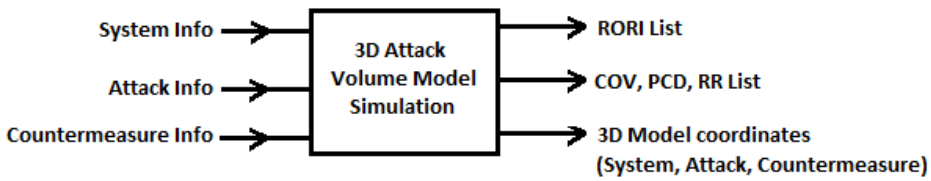


Figure 5.8. 3D Attack Volume Model Simulation

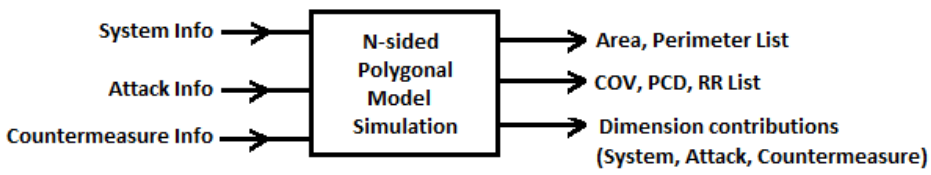


Figure 5.9. N-Sided Polygonal Model Simulation

5.4. Graphical Interfaces

Visualization part of the tool is graphical interfaces. From starting with information data to simulation results, all implementations are about computations and conversions between data structures. In other words, process up until now still has high complexity and understandable for computers. To be able to join human expertise, tool should display more human readable output with visual assistance. For this purpose, drawing implementations are made with respect to geometric models. Figure 5.10 expresses 3D Attack Volume Model by referencing Figure 4.1. Display has a live update with different RCU informations. Adding new attacks to the system or choosing another countermeasure updates visual representation. Red prisms are units under attack and blue ones are protected units by countermeasures. Intersection of these prisms indicates coverage volume of a countermeasure over an attack.

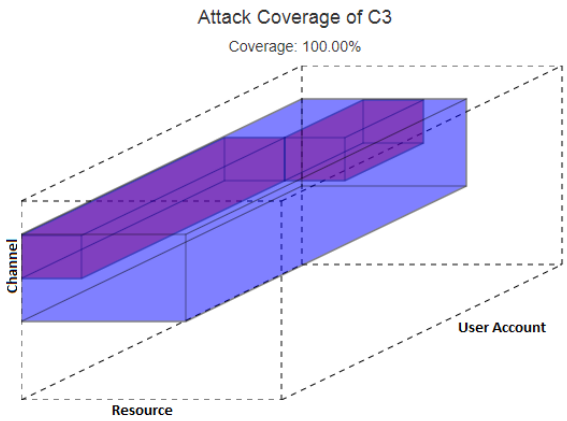


Figure 5.10. 3D Attack Volume Model Display

Similar approach is also used for Figure 5.11. Representations of RCU information is done by drawing events at the system as polygons when n equals 3 similarly to Figure 4.2. Dimension axes have $360/n$ degrees angle between each other. Each dimension contribution value is pointed on axes, then they're connected with lines. Outcome is a polygon which represents an event at the system. Red polygons show attack events and blue ones are countermeasure events.

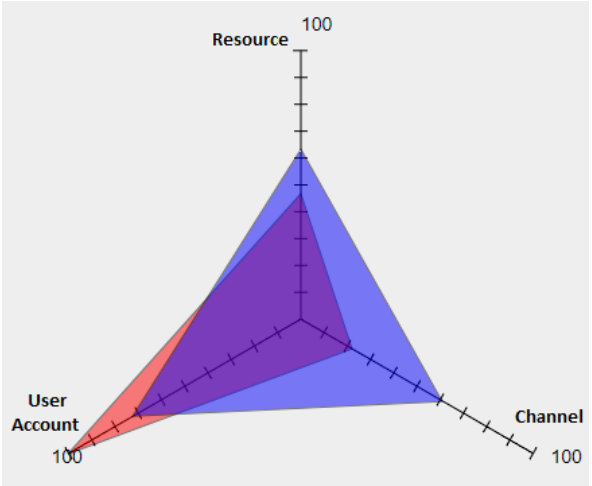


Figure 5.11. N-Sided Polygonal Model Display (n=3)

All implementation of the tool consists of data models, engines, simulations and graphical interfaces. Each part of them has a connection with other parts. Either it's included in other part or it has a input and output relation with other parts. Overall form of the implementation is displayed at Figure 5.12.

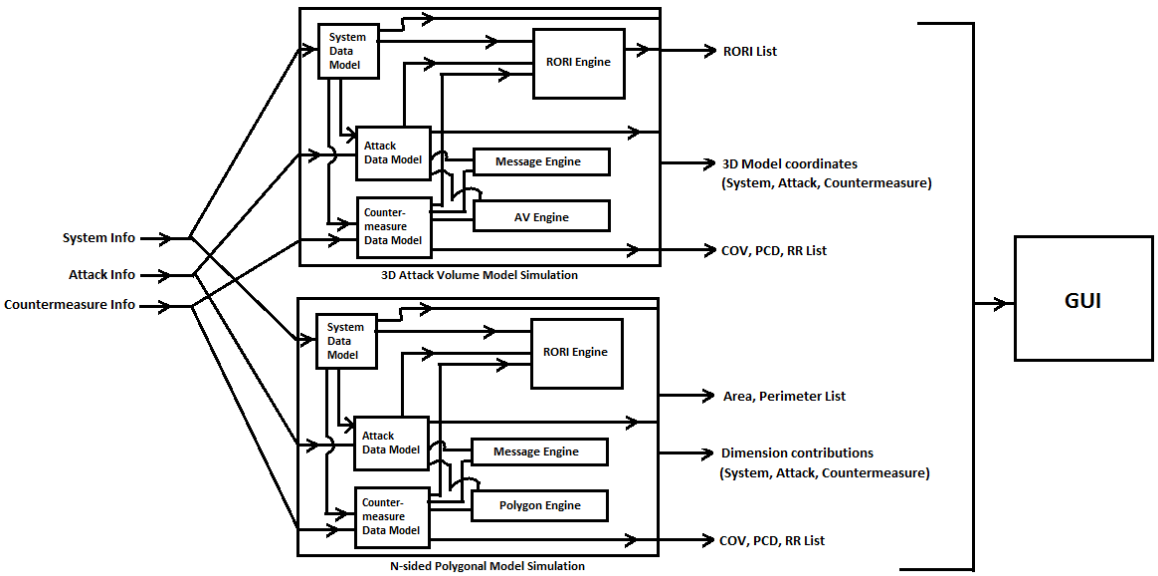


Figure 5.12. Block Diagram of the tool

6. EXPERIMENTS AND RESULTS

Outcome of the implementation is a simulation tool that is constructed as an open platform at [19]. After the tool is opened on an Internet browser, desired simulation scenarios can be executed on the tool by any user or organization. For example, a hacked user account that access to the database of given organization can be an entry point of an attack. Using that account's authentication, a person can make a copy then delete whole information at the database. In this example, database is a logical resource, secure connection between user and database is communication channel and acquired authentication is user account in the system. Potential countermeasures to solve this issue are limiting the access of suspicious account and restore backup of the database. Scenarios which may be similar to these can be tested with the tool by satisfying organization specific needs. Tool has many interactive features to be used by graphical user interfaces. Additionally, visualizations of geometric models and informative numeric data given with tables. Following sections explains these aspects of the tool.

6.1. Interactive features of the tool

There are three tabs which provides different type of interactions in the tool. First one shows information of the system, attacks and countermeasures. RCU information of the system given as at the Table 4.1. Complete value of an infrastructure which is summation of every $units^3$ in the system and AIV are adjustable. Default attacks are at the tool is given at Table 6.1 and default countermeasures are at the Table 6.2. Those events represented as strings of the affected units. All of these events are adjustable. They can be deleted or new ones can be added to create new experiments at the simulation environment. Second tab at the tool displays visualization of attack volume model for chosen countermeasure scenarios. Changing chosen countermeasure affects shown volumes at 3D representation of the system. Third tab has similar features but it's for n-sided polygonal model. Different countermeasure options can be displayed as triangular also with given attacks at the system.

Table 6.1. Attack Strings

Attack Code	**Attack String**	**ARO**
A1	R(1)C(3)U(1-3)	12
A2	R(2)C(3)U(4-6)	12

Table 6.2. Countermeasure Strings

Countermeasure Code	**Countermeasure String**	**EF**
C1	R(1)C(3)U(1-3)	0.8
C2	R(1-3)C(1-2)U(1-3)	0.7
C3	R(1-3)C(2-3)U(1-6)	0.38

6.2. Results of Attack Volume Model

Example information of the simulation can be gathered from Table 4.1, 6.1 and 6.2. Those have relevant data to execute a simulation in the tool. In addition to those, it should be given AIV and complete infrastructure value. As default values, complete infrastructure value is chosen 4500 and AIV is chosen 700. First, system volume and CF is found by using system data model. (4.1) and (4.2) helps calculation as following:

$$SV(S) = (2\times7+2\times5+2\times3)\times(1\times9+2\times5+2\times2)\times(2\times9+2\times8+2\times1) = 24840 units^3$$

$$CF = 4500/2840 = 0.1811\ \$/units^3$$

where CF is calculated by division of complete infrastructure value and system volume. Similarly, total attack volume is calculated as $AV(A) = AV(A_1) + AV(A_2) =$

1260 $units^3$ by (4.3). ALE is found with CF, AV(A) and ARO as following:

$$ALE = CF \times AV(A) \times ARO = 0.1811 \times 1260 \times 12 = 2739\ \$$$

where $CF \times AV(A)$ gives SLE of the combination of attacks at the system. Now, it's assumed countermeasure C1 at Table 6.2 is chosen for the protection of the system. It's needed to calculate ARC and RM of the chosen countermeasure by the data above and countermeasure data model. ARC is assumed to be correlated with how many units are affected by the countermeasure so CF times $CV(C)$ gives annual response cost for protection option.

$$ARC = CF \times CV(C_1) = 0.1811 \times 910 = 164\ \$$$

where $CV(C)$ is calculated via (4.4). Coverage of the countermeasure C1 and RM are last parameters that need to be calculated. COV is found 72.22% by (4.5) and $RM = 0.7222 \times 0.8 = 0.58$ is by (3.3). RR and PCD are also calculated for additional information about countermeasure by using (5.1) and (5.2). They're 27.78% and 0% respectively. With the all calculated parameters, RORI index of C1 countermeasure is as following:

$$RORI(C_1) = \frac{(2739 \times 0.58) - 164}{164 + 700} \times 100 = 163.930$$

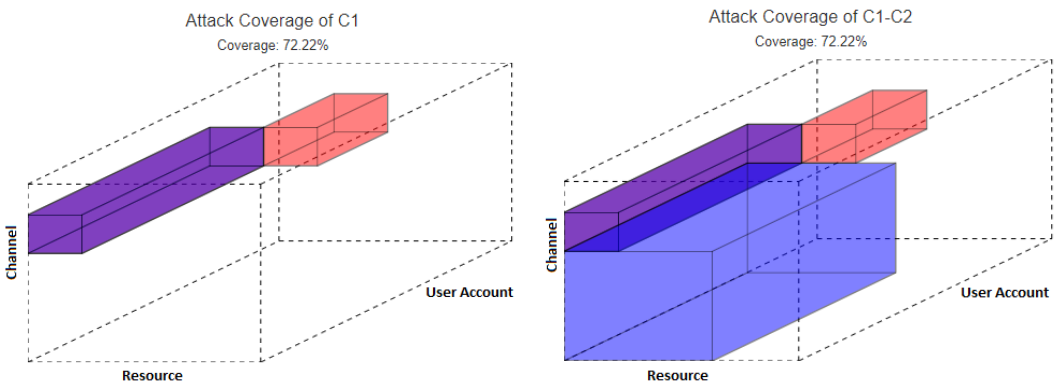
All combinations of countermeasure options are considered to find RORI indexes of them. Calculations above are repeated for other combinations as well. Only difference is that if there are more than one countermeasure, $CV(C)$ is union of countermeasure volumes and minimum EF of them is chosen. Table 6.3 displays all RORI indexes with given example dataset.

Addition to metric data, each countermeasure option can be observed with the system volume and attack volumes like Figure 6.1 expresses. Red color is used for

units under attack and blue is for units that are protected by countermeasure. Figure 6.1(a) is a single countermeasure C1 and Figure 6.1(b) is a combination of C1 and C2 countermeasure options. Figure 6.2 has also similar properties but it shows the units by scatter plotting. Each point at the figure represents intersection of units in 3 dimensions. Because different units have different weights, each point has different value for resulted volume in the system with the unit of $units^3$.

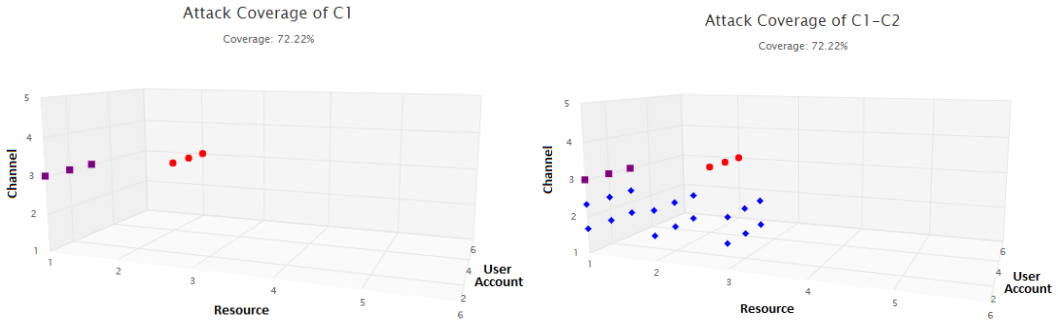
Table 6.3. Results of Attack Volume Model

Code	**RORI Index**	**Coverage**	**RR**	**PCD**
C1	163.930	72.22%	27.78%	0%
C2	-64.156	0%	100%	100%
C3	-10.224	100%	0%	81.58%
C1-C2	-1.557	72.22%	27.78%	88.37%
C1-C3	-10.224	100%	0%	81.58%
C2-C3	-36.570	100%	0%	88.84%
C1-C2-C3	-36.570	100%	0%	88.84%



(a) C1 (b) C1-C2

Figure 6.1. Attack Coverage of C1 and C1-C2



(a) C1 (b) C1-C2

Figure 6.2. Attack Coverage of C1 and C1-C2 with scatter plotting

6.2.1. Graph Representations of Results

The tool supports few graphs to compare crucial parameters of the system. Decision on importance of parameters is given according to optimum outcomes and cost limitations. Chosen parameters are COV, ARC and RORI index. Organizations should aim higher coverage for the system under attack. However, increase in coverage needs higher investment. ARC is directly related to investment amount. Lowering the ARC is good for organizations. It can be said that ARC is a limitation for the security investment. If there's no budget to activate a countermeasure, it's highly possible to see lowest coverage scores. As it defined earlier, RORI index is an indicator of optimum countermeasure option and it provides to compare effectiveness of countermeasures between each other. But it depends many other parameters. That's why tool also provides graphs of COV and ARC additionally.

Figure 6.3 shows COV and ARC pairs of countermeasure options from Table 6.3. Costs are listed increasingly. According to given countermeasure scenarios of the system, this graph may differ. With example data of the tool, it can be said that coverage are not always related with the cost. When chosen countermeasure does not intersect with the attack, coverage is zero even though such countermeasure causes to organization spending money on it.

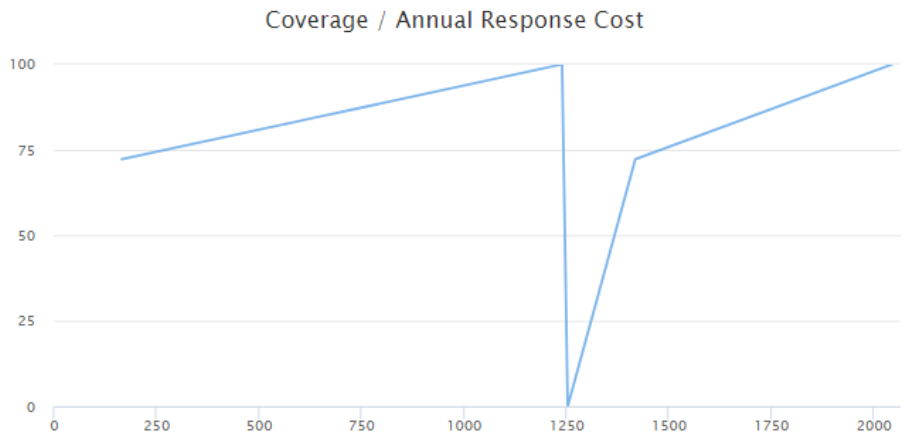


Figure 6.3. Coverage / Annual Response Cost

Figure 6.4 and Figure 6.5 have similar properties. First of all, if a company can spend more money i.e. increase its security investment, it can get better coverage and RORI index scores. This statement can be seen by looking at these figures. Upper limit of ARC affects both COV and RORI index in positive way.

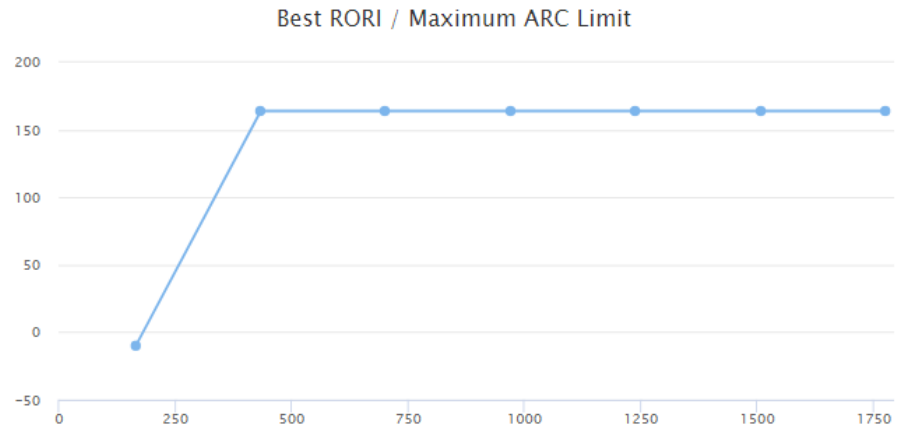


Figure 6.4. Best RORI Index / Maximum ARC Limit

When the constraint is desired coverage percentage rather than amount of money that spent on a countermeasure, Figure 6.6 and Figure 6.7 represent effects of such concerns. It can be said that up to some point it's good to ensure a coverage percentage. However, increase the minimum threshold of coverage causes a burden on organization's budget by increasing ARC. This is also resulted with lower RORI indexes which

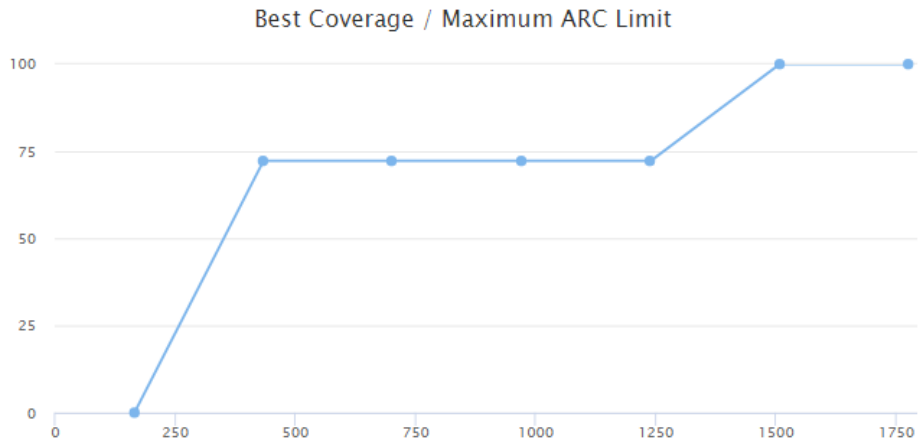


Figure 6.5. Best Coverage / Maximum ARC Limit

indicates non-optimal solutions.

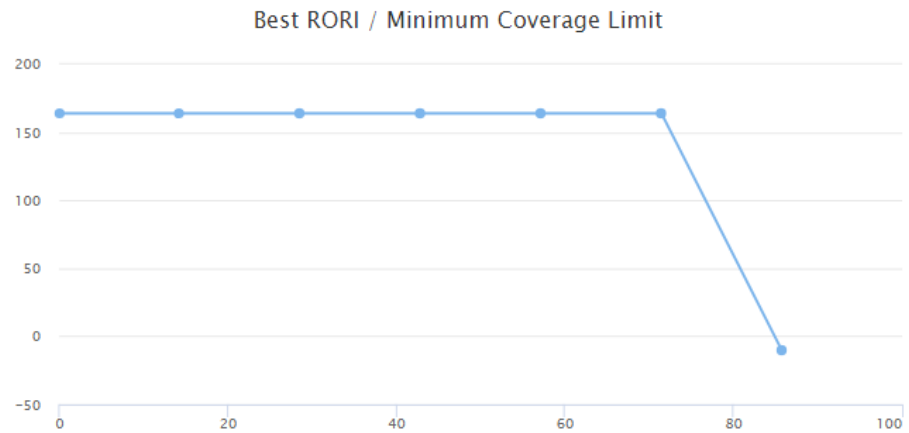


Figure 6.6. Best RORI Index / Minimum Coverage Limit

6.3. Results of N-sided Polygon Model

For N-sided Polygonal Model, information of the system, attacks and countermeasure are same with the simulation of Attack Volume Model. Using the same data for two simulations makes comparative assessment to decide best countermeasure option. This model is based on calculating dimension contributions. Every event which can be an attack or countermeasure has dimension contribution with respect to the

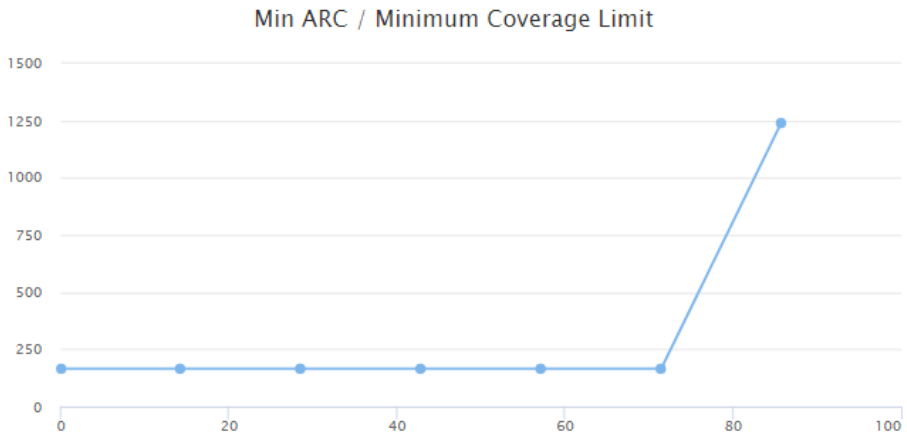


Figure 6.7. Minimum ARC / Minimum Coverage Limit

system. These are used to define a polygon at 2D. With the data used, n equals 3 and every event has a geometric shape of triangular. COV, RR and PCD percentages can be also found with this model. Additionally, perimeter and area of the triangular is given due to examining effectiveness of a countermeasure. Even though, RORI index calculation can be adapted to this model in theory, this study did not calculate RORI index with N-sided Polygonal Model.

Starting with the system's perimeter and area, as a default, the system covers whole range of dimensions so dimension contributions are 100 for each axis. Due to equal angle between dimensions, it's simple geometric problem to find lengths of a triangular. Each length is $100\sqrt[2]{3}$ $unit$ and perimeter is approximately 520 $units$. Area can be found as a 15000 $units^2$ by (4.8). An event's dimension contributions can be calculated by (4.6). As an example, C1's dimension contributions are as following:

$$Co(Resource, C_1) = \frac{1 \times 7}{(2 \times 7) + (2 \times 5) + (2 \times 3)} \times 100 = 23 \ units$$

$$Co(Channel, C_1) = \frac{1 \times 5}{(1 \times 9) + (2 \times 5) + (2 \times 2)} \times 100 = 22 \ units$$

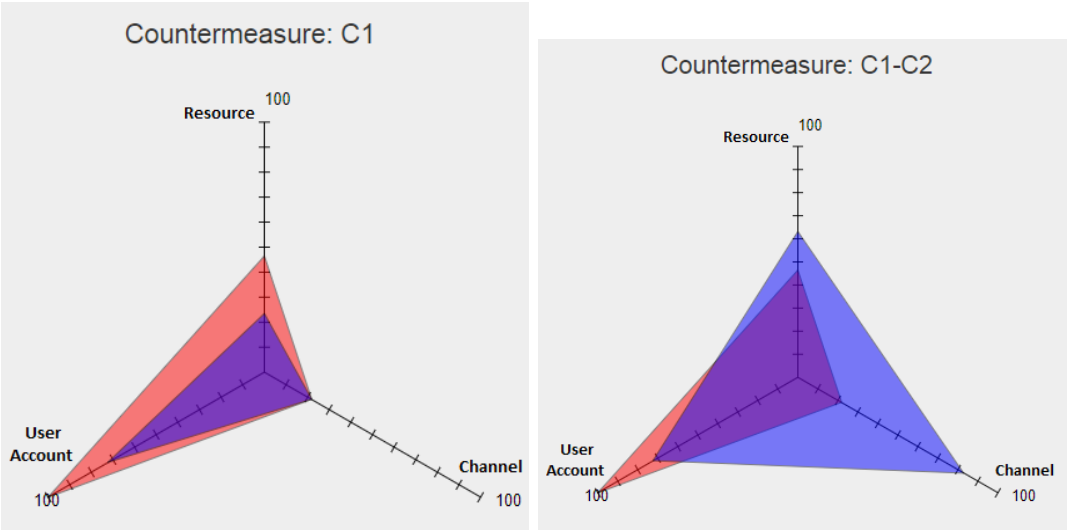
$$Co(UserAccount, C_1) = \frac{(2 \times 9) + (1 \times 8)}{(2 \times 9) + (2 \times 8) + (2 \times 1)} \times 100 = 72 \; units$$

By using (4.7) and (4.8), C1's perimeter is 211 *units* and its area is 1881 $units^2$. Coverage depends on area of intersection of countermeasure and attack. Tables 6.4 shows all results of N-sided polygonal model when n equals 3 with the given dataset. Each row is found by that event's dimension contributions.

Table 6.4. Results of N-sided Polygonal Model

Code	**Perimeter**	**Area**	**Coverage**	**RR**	**PCD**
System	520 *units*	15000 $units^2$			
Attack	303 *units*	3928 $units^2$			
C1	211 *units*	1881 $units^2$	47.89%	52.11%	0%
C2	340 *units*	6413 $units^2$	42.90%	57.10%	73.73%
C3	363 *units*	6717 $units^2$	100%	0%	41.52%
C1-C2	378 *units*	7886 $units^2$	75.79%	24.21%	62.25%
C1-C3	363 *units*	6717 $units^2$	100%	0%	41.52%
C2-C3	428 *units*	9913 $units^2$	100%	0%	60.38%
C1-C2-C3	428 *units*	9913 $units^2$	100%	0%	60.38%

Figure 6.8 shows visual representations of n-sided polygon model in the tool. Cumulative countermeasure options are increases the affected perimeter and area when their union is not equal to one of them. Even though, numeric data are more reliable for decision making, such figures makes easy to imagine effect of chosen solution in the system.



(a) C1 (b) C1-C2

Figure 6.8. Attack Coverage of C1 and C1-C2

7. CONCLUSION AND FUTURE WORK

Implementation of analysis application and using geometric models in the simulation reveal some outcomes. First of all, geometric models make system security and effects on it more understandable. This situation provides visual evidences to system security teams and managers for decision processes. Countermeasure investment options would be more trustworthy with relevant supportive data. The open platform displays how the variables of the system affects numerical data such as RORI index, attack coverage percentage and annual response cost by using simulation of the data. To be able to find desired investment scenario, countermeasure dimensions should be minimized after minimum attack coverage is satisfied. A countermeasure that has broader dimensions than it is needed causes unwanted cost increase for organizations. Trying combinations of countermeasure options is useful to increase viable scenarios and to find best solution amongst them. Finally, it's promising to use the platform in a real world optimization because the simulation succeed to display potential benefits of the applied theory.

There are more steps which can be implemented in future. Currently, two geometric models is implemented and simulated with platform application. However, N-sided Polygonal Model did not combine with RORI index measurement. Implementing RORI index by defining the system as a polygon can be another addition for the tool. With an additional model at [20], attacks and countermeasure at the system can be displayed in a form of prism. Floor of prism is described as n-sided polygon and its height varies according to what type of attack or countermeasure is chosen for display. Such adjustment increases quality of comparative assessment between geometric models. Applying all there geometric models to find necessary countermeasure can provide more trusted solution options.

Current implementation uses default parameters for the system, attacks and countermeasures at start. Tool can be used as a black box that can get input from organizations or individual users and it gives output metrics and visualizations to them.

For such purpose, platform application should provide an application programmable interface (API) for third parties. Authorized parties should send their data by secure channel and get outcomes to their domain. Outcomes can be received by their client program or be sent as an e-mail to their security experts. Software as a service (SaaS) is an example of this type of usage. Third parties can use the platform application as a service for choosing optimum countermeasure to secure their systems. SaaS approach also changes to context to dynamic countermeasure selection in real time. Continuous flow of data to application provides live selection of countermeasure for organizations. For example defending DDoS attacks like mentioned in [21] achievable by future implementations of the application.

Lastly, rather than considering economic aspects of the countermeasures, outcomes of selection may lead to improve policy management at the system. At identity access management systems similar to in [22], policy enforcement points can be adaptive according to collection of chosen countermeasure scenarios. Attack detection triggers countermeasure selection then selected solution affects used policies in the system.

REFERENCES

1. Gortney, W. E., *Department of Defense Dictionary of Military and Associated Terms*, Tech. rep., Joint chiefs Of Staff Washington United States, 2010.

2. Shameli-Sendi, A., R. Aghababaei-Barzegar and M. Cheriet, "Taxonomy of information security risk assessment (ISRA)", *Computers & security*, Vol. 57, pp. 14–30, 2016.

3. Díaz-López, D., G. Dólera-Tormo, F. Gómez-Mármol and G. Martínez-Pérez, "Dynamic counter-measures for risk-based access control systems: An evolutive approach", *Future Generation Computer Systems*, Vol. 55, pp. 321–335, 2016.

4. Gonzalez-Granadillo, G., J. Garcia-Alfaro, E. Alvarez, M. El-Barbori and H. Debar, "Selecting optimal countermeasures for attacks against critical systems using the attack volume model and the RORI index", *Computers & Electrical Engineering*, Vol. 47, pp. 13–34, 2015.

5. Baca, D. and K. Petersen, "Countermeasure graphs for software security risk assessment: An action research", *Journal of Systems and Software*, Vol. 86, No. 9, pp. 2411–2428, 2013.

6. Kolomeec, M., G. Gonzalez-Granadillo, E. Doynikova, A. Chechulin, I. Kotenko and H. Debar, "Choosing Models for Security Metrics Visualization", *International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security*, pp. 75–87, Springer, 2017.

7. Granadillo, G. G., A. Motzek, J. Garcia-Alfaro and H. Debar, "Selection of mitigation actions based on financial and operational impact assessments", *Availability, Reliability and Security (ARES), 2016 11th International Conference on*, pp. 137–146, IEEE, 2016.

8. Gonzalez-Granadillo, G., J. Rubio-Hernan and J. Garcia-Alfaro, "Using an event data taxonomy to represent the impact of cyber events as geometrical instances", *IEEE access*, Vol. 6, pp. 8810–8828, 2018.

9. Kotenko, I. and E. Doynikova, "Dynamical calculation of security metrics for countermeasure selection in computer networks", *Parallel, Distributed, and Network-Based Processing (PDP), 2016 24th Euromicro International Conference on*, pp. 558–565, IEEE, 2016.

10. Kotenko, I. and E. Doynikova, "Selection of countermeasures against network attacks based on dynamical calculation of security metrics", *The Journal of Defense Modeling and Simulation*, Vol. 15, No. 2, pp. 181–204, 2018.

11. Chung, C.-J., P. Khatkar, T. Xing, J. Lee and D. Huang, "NICE: Network intrusion detection and countermeasure selection in virtual network systems", *IEEE transactions on dependable and secure computing*, Vol. 10, No. 4, pp. 198–211, 2013.

12. Gonzalez-Granadillo, G., S. Dubus, A. Motzek, J. Garcia-Alfaro, E. Alvarez, M. Merialdo, S. Papillon and H. Debar, "Dynamic risk management response system to handle cyber threats", *Future Generation Computer Systems*, 2017.

13. Granadillo, G. G., M. Belhaouane, H. Debar and G. Jacob, "RORI-based countermeasure selection using the OrBAC formalism", *International journal of information security*, Vol. 13, No. 1, pp. 63–79, 2014.

14. Mont, M. C., Y. Beresnevichiene, D. Pym and S. Shiu, "Economics of identity and access management: Providing decision support for investments", *Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP*, pp. 134–141, IEEE, 2010.

15. Kheir, N., N. Cuppens-Boulahia, F. Cuppens and H. Debar, "A service dependency model for cost-sensitive intrusion response", *European Symposium on Research in*

Computer Security, pp. 626–642, Springer, 2010.

16. Granadillo, G. G., J. Garcia-Alfaro and H. Debar, "Using a 3D geometrical model to improve accuracy in the evaluation and selection of countermeasures against complex cyber attacks", *International Conference on Security and Privacy in Communication Systems*, pp. 538–555, Springer, 2015.

17. Gonzalez-Granadillo, G., J. Garcia-Alfaro and H. Debar, "An n-sided polygonal model to calculate the impact of cyber security events", *International Conference on Risks and Security of Internet and Systems*, pp. 87–102, Springer, 2016.

18. Rentsch, T., "Object oriented programming", *ACM Sigplan Notices*, Vol. 17, No. 9, pp. 51–57, 1982.

19. Bal, O., *Open Platform for Attack and Countermeasure Analysis on System Security*, 2018, `https://ozgunbal.github.io/countermeasure-selection-tool`, accessed at May 2018.

20. González-Granadillo, G., J. Rubio-Hernan, J. Garcia-Alfaro and H. Debar, "Considering internal vulnerabilities and the attacker's knowledge to model the impact of cyber events as geometrical prisms", *Trustcom/BigDataSE/I SPA, 2016 IEEE*, pp. 340–348, IEEE, 2016.

21. Xiang, Y., W. Zhou and Z. Li, "An analytical model for DDoS attacks and defense", *Computing in the Global Information Technology, 2006. ICCGI'06. International Multi-Conference on*, pp. 66–66, IEEE, 2006.

22. Hummer, M., M. Kunz, M. Netter, L. Fuchs and G. Pernul, "Adaptive identity and access management—contextual data based policies", *EURASIP Journal on Information Security*, Vol. 2016, No. 1, p. 19, 2016.