Network Threat Characterization in Multiple Intrusion Perspectives using Data Mining Technique

[1]Oluwafemi Oriola, [2]Adesesan B. Adeyemo and
[3]Oluwaseyitanfunmi Osunade

[1]Department of Computer Science, University of Ibadan, Ibadan, Nigeria
oluwafemioriola@yahoo.com
[2]Department of Computer Science, University of Ibadan, Ibadan, Nigeria
sesan_adeyemo@yahoo.com
[3]Department of Computer Science, University of Ibadan, Ibadan, Nigeria
o.osunade@mail.ui.edu.ng

ABSTRACT

For effective security incidence response on the network, a reputable approach must be in place at both protected and unprotected region of the network. This is because compromise in the demilitarized zone could be precursor to threat inside the network. The improved complexity of attacks in present times and vulnerability of system are motivations for this work. Past and present approaches to intrusion detection and prevention have neglected victim and attacker properties despite the fact that for intrusion to occur, an overt act by an attacker and a manifestation, observable by the intended victim, which results from that act are required. Therefore, this paper presents a threat characterization model for attacks from the victim and the attacker perspective of intrusion using data mining technique. The data mining technique combines Frequent Temporal Sequence Association Mining and Fuzzy Logic. Apriori Association Mining algorithm was used to mine temporal rule patterns from alert sequences while Fuzzy Control System was used to rate exploits. The results of the experiment show that accurate threat characterization in multiple intrusion perspectives could be actualized using Fuzzy Association Mining. Also, the results proved that sequence of exploits could be used to rate threat and are motivated by victim properties and attacker objectives.

KEYWORDS

Intrusion Prevention, Temporal Sequence Patterns, Association Mining, Fuzzy Logic & Perspective of Intrusions

1. INTRODUCTION

The insurgence of threats most especially new threats on the internet calls for serious concern. These threats target assets both in the inside and the demilitarize zone (DMZ) of the networks. In fact, availability of reputable security set up at the demilitarize zone will improve security at the inside zone. While the assets in the inside zone are protected by inside firewall, application firewall inclusive, the asset in the DMZ could benefit from outside zone firewall. This is in line with Intrusion Prevention System goal [2] of detecting intrusions and responding to the intrusions actively using firewall. A simple representation of the analogy is presented in Figure 1.

Defining what constitutes an attack is difficult because multiple perspectives are involved. Attacks may involve any number of attackers and victims. The attacker's viewpoint is typically characterized by intent and risk of exposure. From a victim's perspective, intrusions are characterized by their manifestations, which may or may not include damage. Some attacks may produce no manifestations, and some apparent manifestations may result from system and

DOI : 10.5121/ijnsa.2012.4611

network malfunctions. Some attacks involve the involuntary participation of additional machines, usually victims of earlier attacks. For an intrusion to occur, it requires both an overt act by an attacker and a manifestation, observable by the intended victim, which results from that act [10].

A victim's view of an attack is usually focused on these manifestations:

- *What happened?*
- *Who is affected and what were the consequences?*
- *Who is the intruder?*
- *Where and when did the intrusion originate?*
- *How and why did the intrusion happen?*

Meanwhile, the attacker may have quite a different view*:*

- *What is my objective?*
- *What vulnerabilities exist in the target system?*
- *What damage or other consequences are likely?*
- *What exploit scripts or other attack tools are available?*
- *What is my risk of exposure?*

While victim's view of the attacks emphasizes on who the attacker is and what happened, attacker centric emphasizes on what attackers could do and their objectives. These perspectives were used independently in [12] that different properties of the victim effectuate different ways for an attacker to compromise a system and [1] position that different attackers institute different attack strategies based on capabilities and objectives.

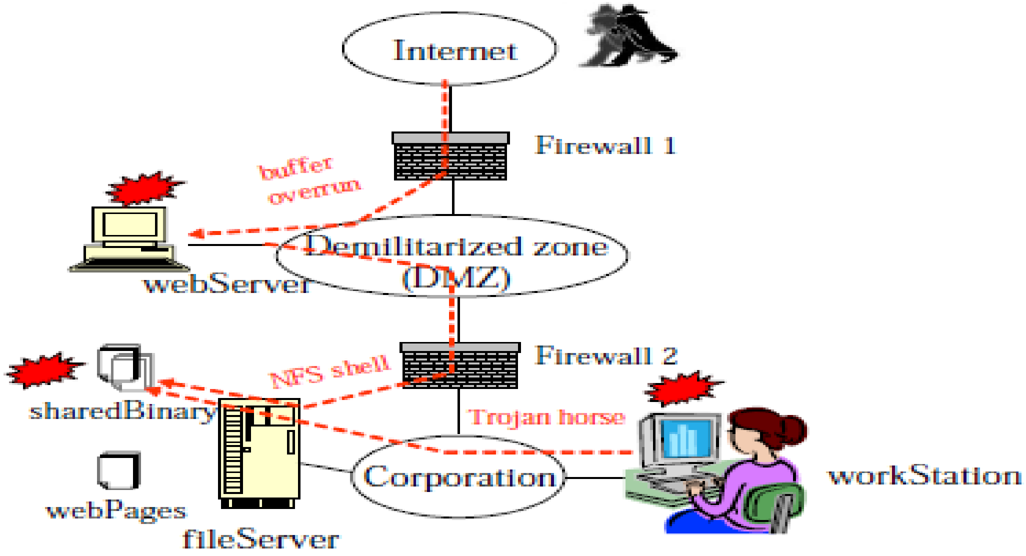


Figure 1: An Internet Set up showing Assets, Threats and Firewalls

Therefore, in order to successfully militate against attacks in the network most especially in situation of intrusion prediction, a reliable incidence response mechanism for defence against attacks from attackers and victim point of view is required. This will culminate in extensive analysis of events, accurate prediction and real time prevention of eventualities. That is, real time proactive response can be issued as there will not be need to carry out any analysis of event at the response segment. We present techniques to automatically rate threats from intrusion alerts generated by Intrusion Detection System (IDS).

2. RELATED WORKS

Several works have been carried out on threat modelling in computer networks. These works will be reviewed under network attack strategy analysis and risk assessment.

Many of the works on attack strategy analysis concentrated on attack graph modelling. According to [14], a network attack graph is a state transition diagram in which each state represents a state of the attacker, the defender and the system. Transitions in an attack graph represent actions taken by an attacker which results in a change in the state of the entire system [9]. An action from the attacker may lead to the state which is the attacker's goal. If the system is in a final state, it means that the attacker has succeeded in exploiting the system. An action from a defender team can void the actions of the attacker and can lead to previous safer states. [9] suggested a data mining based approach to generate attack graphs. The purpose of their work is to use data mining to construct attack graphs. There is a casual relationship between an attacker and the alert raised by IDS. They performed data mining on intrusion alerts to find association rules from the dataset.

In [3], pre and post-conditions were defined for individual attacks, and alerts were connected (or correlated) when the post-condition of one alert matches the precondition of a later one. This allowed for the specification of complex chains of attacks without having to explicitly model complex scenarios. For an example of an attack that can be correlated using this technique, they considered an attack where the intruder first breaks into a host in the Demilitarized Zone (DMZ) of a company. A demilitarized zone is a computer network that sits between the internal network and the Internet and acts as a security bufferer. After breaking into this host, the attacker performs another attack starting from the compromised host. Both steps of the attack were captured by attack graph. [1] suggested that one method for handling attack graph complexity and scalability is to differentiate between likely and unlikely attack paths using threat modelling. Their approach used a decision model to identify the most probable attack path using threat modelling.

In risk assessment researches in network systems, [12] posited that security risk assessment and mitigation are two vital processes that need to be executed to maintain a productive information technology infrastructure. They resolved that other risk assessment models have not helped to reason about the causal dependencies between network states. Further, the optimization formulations ignore the issue of resource availability while analyzing a risk model. Hence, their paper proposed a risk management framework using Bayesian networks that enable a system administrator to quantify the chances of network compromise at various levels. Also, [5] proposed fuzzy system approach to rank vulnerability based on the possible risk of network assets. However, quantifying network assets in terms of possible risk is not trivial. Therefore, their work was impractical. Another work with the same demerit on fuzzy risk assessment in distributed system was carried out by [6].

3. MATERIALS AND METHODS

This following presents some of the techniques used in this work for network threat characterization.

3.1 Data Mining

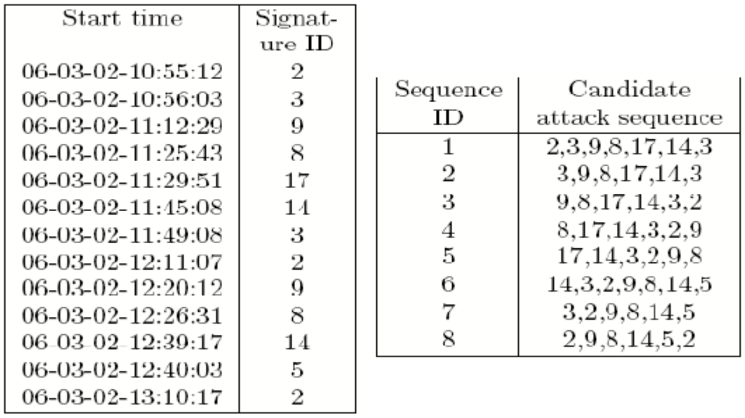
Data Mining refers to the nontrivial extraction of implicit, previously unknown and potentially useful information from data in databases [15]. It is a key step of Knowledge Discovery from Databases (KDD). In other words, Data Mining involves the systematic analysis of large data sets using automated methods which are mostly statistical, machine learning and soft computing based. By probing data in this manner, it is possible to prove or disprove existing hypotheses or ideas regarding data or information, while discovering new or previously unknown information. It is noted for its Pattern Recognition ability that ensures that information is obtained from vague data. The data mining procedure used for our work involves the following steps:

- *Alert Cleansing*
- *Transformation of Alert into Attack Sequence using a pre-specified Time Window.*
- *Frequent Association Mining of the Sequence*
- *Threat Rating Using Fuzzy Control System*
- *Interpretation of results*

3.2 Frequent Sequence Temporal Patterns

Once the alerts are recorded in the database, the next step is to process the alert information and prepare it for the next step of the processing. The alerts have signature id and timestamp information with it. Each Signature ID could be an integer number or letters and indicates a different type of an attack. The whole intrusion alerts are sorted in ascending order by their timestamp in sequence. This is called global attack sequence.

The “Attack Sequence Time Window” [9] is the time interval which is moved along the global attack sequence. Attack Sequence Time Window is presented in Figure 2. In this step, the global sequence of attacks is broken down into smaller attack.



Start time	Signat-ure ID
06-03-02-10:55:12	2
06-03-02-10:56:03	3
06-03-02-11:12:29	9
06-03-02-11:25:43	8
06-03-02-11:29:51	17
06-03-02-11:45:08	14
06-03-02-11:49:08	3
06-03-02-12:11:07	2
06-03-02-12:20:12	9
06-03-02-12:26:31	8
06-03-02-12:39:17	14
06-03-02-12:40:03	5
06-03-02-13:10:17	2

(a) Sample Alert Database

Sequence ID	Candidate attack sequence
1	2,3,9,8,17,14,3
2	3,9,8,17,14,3
3	9,8,17,14,3,2
4	8,17,14,3,2,9
5	17,14,3,2,9,8
6	14,3,2,9,8,14,5
7	3,2,9,8,14,5
8	2,9,8,14,5,2

(b) Candidate Attack Sequences

Figure 2. Alert Sequences Sources: [9]

3.3 Apriori Algorithm

The algorithm is used to find the *frequent itemsets* that is the sets of sequence that have minimum support. The minimum support is used to generate association rules. The pseudocode is presented as follows:

```
Ck: Candidate itemset of size k
Lk: frequent itemset of size k
L1= {frequent items};
for(k= 1; Lk!=□; k++) do begin
Ck+1= candidates generated from Lk;
for each transaction t in database $d_o$
increment the count of all candidates in Ck+1 that are contained in t
Lk+1= candidates in Ck+1with min_support
return □kLk;
```

Confidence (A =>B) = (Tuples containing both A and B) / (Tuples Containing A)   Eq. 1

3.4 Fuzzy Control System

Fuzzy control replaces the role of the mathematical model in cases of imprecision. It depends on rule set obtainable from experts in the domain of discourse. The process of inference is used to bind inputs together to produce the desired outputs.

The general inference process proceeds in four steps:

a. *Fuzzification*, the membership functions defined on the input variables are applied to their actual values, to determine the degree of truth for each rule premise.
b. *Inference*, the truth value for the premise of each rule is computed, and applied to the conclusion part of each rule. This results in one fuzzy subset to be assigned to each output variable for each rule. We use *Min* as inference rules.
c. *Composition*, all of the fuzzy subsets assigned to each output variable are combined together to form a single fuzzy subset for each output variable. We use

   Root Sum Square = $\sqrt{\sum^{n}_{i=1} X_{ij}^{2}}$ Eq. 2

   for i = membership value of input i for j linguistic variables.

d. *Defuzzification*, which is used when it is useful to convert the fuzzy output set to a crisp number. The Centroid value is used.

   Fuzzy Centroid Output = $\sum^{N}_{i=1}(\text{centre}_{i} \, . \, \text{strength}_{i}) / \sum^{N}_{i=1} \text{Strength}_{i}$ Eq. 3

   where N is the number of output members.

3.5 Decision Hierarchy of Criteria and Sub-Criteria of Threat

Attackers perpetrate attacks based on the characteristics of the victim and their objectives. Attackers can be generally divided into Experienced and Novice and/or Opportunist, Hackers, Explorer. To cater for these two widely acceptable taxonomies of attackers [9] [4], we modify [1]Decision Hierarchy of Criteria and Sub-Criteria to include Accessibility criterion with Authentication, and Access Vector sub-criteria in conformity with [11] as presented in Figure 3.

The value high, medium and low is the category of individual threat. In Table 1, we present the Criteria Rating for Threat. An expert adversary always engages in exploits with high intention of success coupled with high consideration for risk of detection. This affects its complexity, therefore accessibility is high. An adversary who falls below the expert category can be an associate or a beginner. If it is an associate, its concern for success and potential damage are high. Its choices of exploit are often sound in theory but poor in practice. A beginner adversary uses trial and error method; therefore, it perpetrates different exploits in order to reach its goal. In fact, it may not even be aware of the goal when it is reached

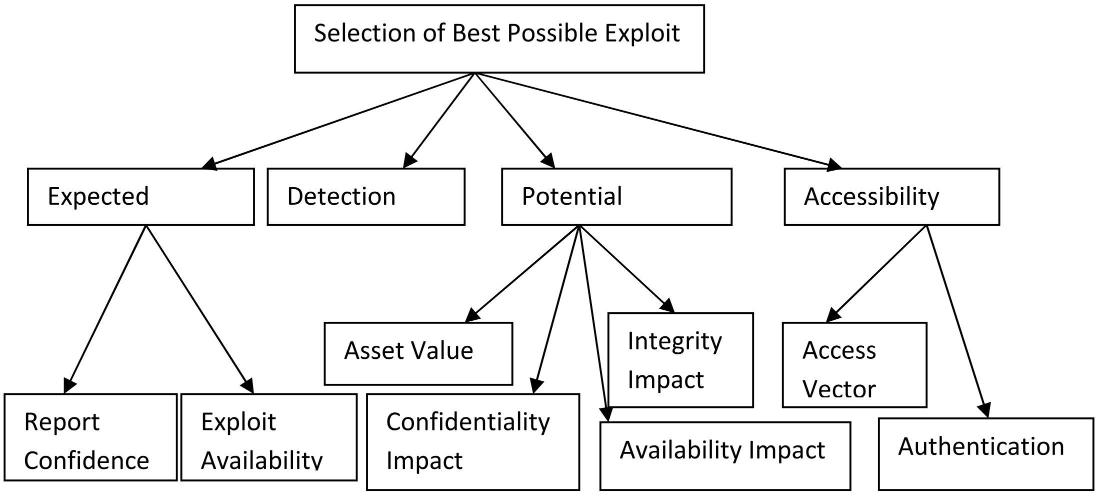


Figure 3: Decision Criteria and Sub-criteria Hierarchy from Attackers Perspective

Table 1: Criteria Rating for Threat

Adversary/Attacker	**Expert**	**Associate**	**Beginners**
Expected Success	High	High	Low
Risk of Detection	High	Low	Low
Potential Damage	Low	High	High
Accessibility	High	Low	Low
Threat Rating	**High/Medium/Low**	**High/Medium/Low**	**High/Medium/Low**

4. MODEL DEVELOPMENT

4.1 Data Preprocessing

We formatted the DARPA 2000 TCPDump Datasets as Inside 1, Inside 2, Outside 1 and Outside 2. The Inside 1 and Inside 2 datasets are the original alerts as generated by SNORT IDS. The Outside 1 and Outside 2 consist of reconstructed combined alerts of Inside 1 and DMZ 1 as Outside 1 and Inside2 and DMZ 2 as Outside 2. The motivation for this is to enable effective incidence response within protected zones and less protected zones of network. Also, in order to generate candidate alert sequences, individual event name was given identification (A, B,..., Z, AA, AB) in total of twenty nine (29) in all and time window was set at 10 Minutes.

4.2 Association Mining Model

The frequent temporal sequence association miner was set at 0.5 confidence level. Table 2, Table 3, Table 4 and Table 5 present the results of the model.

Table 2: Inside Scenario 1 Association Rules

ID	Rules (Support)	Confidence
1	G 83 => F 83	1
2	D, W 110 => D 102	0.93
3	F 96 => G 83	0.86
4	D, D 119 => W 102	0.86
5	W 156 => D 133	0.85
6	W, D 130 => D 101	0.78
7	W 154 => D, D 101	0.66
8	D 207 => W 131	0.63
9	D 207 => D 118	0.57

Table 3: Inside Scenario 2 Association Rules

ID	Rules (Support)	Confidence
1	D, W 38 => D 34	0.89
2	W 48 => D 40	0.83
3	D, D 44 => W 34	0.77
4	D 76 => W 45	0.59
5	D 73 => D 43	0.58
6	W 62 => D, D 34	0.55

Table 4: Outside Scenario 1 Association Rules

ID	Rules (Support)	Confidence
1	G 68 => F 68	1
2	W, D 65 => D 65	1
3	D, W 89 => D 83	0.93
4	F 75 =. G 68	0.91
5	D, D 95 => W 83	0.87
6	W 124 => D 105	0.85
7	W 123 => D, D 83	0.67
8	D 169 => D 98	0.58
9	D 165 => D, W 83	0.5

Table 5: Outside Scenario 2 Association Rules

ID	Rules (Support)	Confidence
1	D, W 36 => D 33	0.92
2	W 47 => D 40	0.85
3	W, D 45 => D 34	0.76
4	D, D 45 => W 34	0.76
5	W 52 => D, D 33	0.63
6	D 75 => D 45	0.6
7	D 75 => W 45	0.6

4.3 Fuzzy Threat Rating

Risk is a function of threat likelihood and potential damage on an asset. However, it is intuitively impossible to get the precise value of these variables. Hence, obtaining the value of risk in precise term is not trivial [5]. Hence, we adopted fuzzy system in modelling threat. In Table 6, a rules matrix consisting of fuzzy rules is presented.

Threat confidence weight is the confidence value of the exploit as generated by the frequent association miner. The linguistic variable set is given as:

$$Input_A = \{Very\ High,\ Moderately\ High,\ Somewhat\ High\}$$

The target input variable set is made up of base scores obtained from National Vulnerability Database CVS (NVD, 2012) whose linguistic variables set is given as

$$Input_B = \{High,\ Moderate,\ Low\}$$

Table 6: Rule Matrix for Threat Rating

Input A/ Input B	**H**	**M**	**L**
VH	M	H	H
MH	L	M	H
SH	L	M	H

Figure 4, Figure 5 and Figure 6 present the membership function triangular shape of the inputs and output

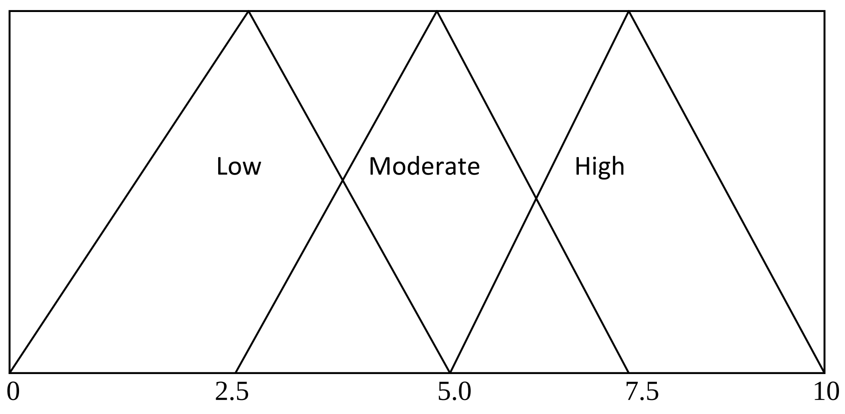


Figure 4: Membership Function of Vulnerability Base Score

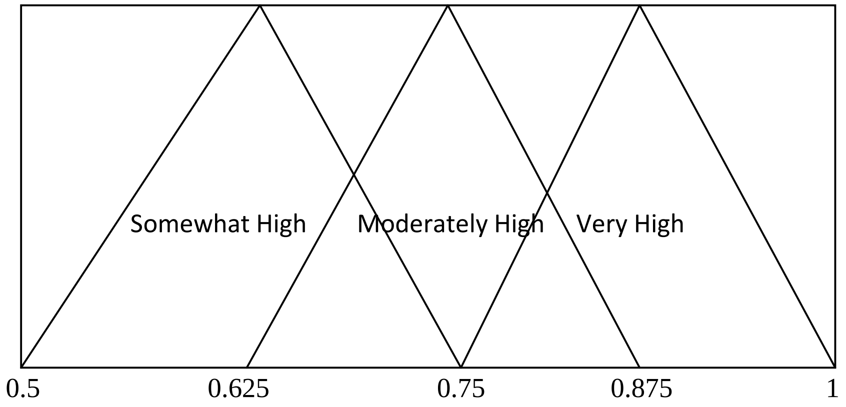


Figure 5: Membership Function of Confidence Value of Exploit

The output or consequence is the Threat Rating whose linguistic variable set is given as:

Output = {High, Medium, Low}

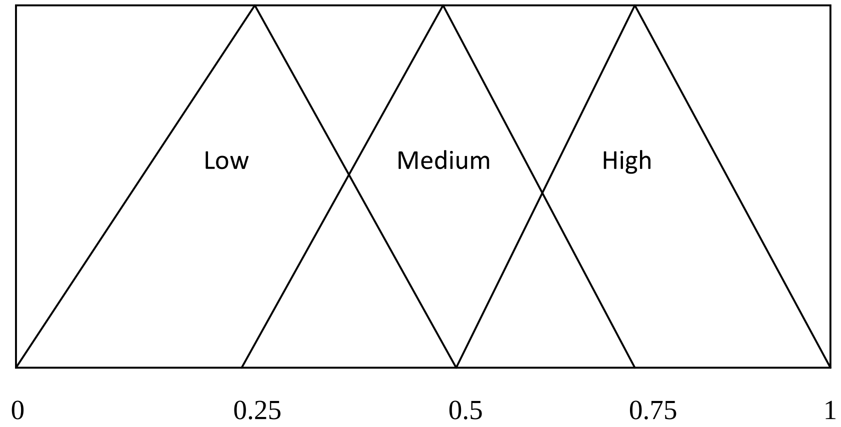


Figure 6: Membership Function of Threat Rating

Table 7: Inside Scenario 1 Exploits Outcome

ID	**Rules**	**Confidence**	**Vulnerability**	**Rating**
1	G => F	1	10	0.5
2	D, W => D	0.93	10	0.5
3	F => G	0.86	10	0.375
4	D, D => W	0.86	10	0.375
5	W => D	0.85	10	0.375
6	W, D => D	0.78	10	0.375
7	W => D, D	0.66	10	0.25
8	D => W	0.63	10	0.25
9	D => D	0.57	10	0.25

Table 8: Inside Scenario 2 Exploits Outcome

ID	**Rules**	**Confidence**	**Vulnerability**	**Rating**
1	D, W => D	0.89	10	0.5
2	W => D	0.83	10	0.375
3	D, D => W	0.77	10	0.375
4	D => W	0.59	10	0.25
5	D => D	0.58	10	0.25
6	W => D, D	0.55	10	0.25

Table 9: Outside Scenario 1 Exploits Outcome

ID	**Rules**	**Confidence**	**Vulnerability**	**Rating**
1	G => F	1	10	0.5
2	W, D => D	1	10	0.5
3	D, W => D	0.93	10	0.5
4	F =. G	0.91	10	0.5
5	D, D => W	0.87	10	0.375
6	W => D	0.85	10	0.375
7	W => D, D	0.67	10	0.25
8	D => D	0.58	10	0.25
9	D => D, W	0.5	10	0.25

Table 10: Outside Scenario 2 Exploits Outcome

ID	**Rules (Support)**	**Confidence**	**Vulnerability**	**Rating**
1	D, W => D	0.92	10	0.5
2	W => D	0.85	10	0.375
3	W, D => D	0.76	10	0.375
4	D, D => W	0.76	10	0.375
5	W => D, D	0.63	10	0.25
6	D => D	0.6	10	0.25
7	D => W	0.6	10	0.25

From the frequent association rules presented in Table 2, Table 3, Table 4 and Table 5, same exploit sequences have different confidence value at different scenarios and zones. This does not reflect the true nature of threats because same threats are expected to have the same characteristics. We attribute this to victim attributes which include among others [12]:

i. system vulnerabilities (as reported in vulnerability databases such as BugTraq, CERT/CC, or netcat),

ii. (insecure) system properties such as unsafe security policy, corrupted file/memory access permission, or read-write access in file structure,

iii. (insecure) network properties such as unsafe network condition, unsafe firewall properties, unsafe device/ peripheral access permission, and

iv. access privilege such as user account, guest account, or root account.

However, in our experimental study on fuzzy model, we found for each group the threat rating, given that the vulnerability base score of the threat is 10 as presented in CVSS [11] [8]. This is practical considering the vulnerability of the systems as reported in DARPA 2000 Scenario Dataset [7] which is typical of an experimental settings used to obtain publicly available intrusion dataset and the fact that there is no system without vulnerability [13]. The threat ratings are the output of the defuzzification step. These threat ratings for the exploits association rules are presented in Table 7, Table 8, Table 9 and Table 10.

The results of the experiments presented in Table 7, Table 8, Table 9 and Table 10 show that at vulnerability base score of 10 with varied confidence value of sequence of exploits, the outcome of fuzzy threat rating for same exploits are equal for all scenarios both inside and outside the network. In fact, at both the inside and the demilitarize zone, the threat rating for same sequence of exploit are the same. This shows that system are not only susceptible to threat in the inside but also at the demilitarize zone. The threat ratings also show that the threat characteristics lie within low and medium range of the threat rating membership category. However, exploits with the threat rating of 0.375 lie between low and medium category of threat unlike exploits with 0.25 and 0.5 which are either low or medium. With reference to criteria rating in Table 1, beginner adversary (or Scenario 1 Attacker) for DARPA 2000 Scenario threats are rated as either low or medium while associate adversary (or Scenario 2 Attacker) for same experiment are also rated either as low or medium. This shows that beginner adversary could perpetrate both medium and low level threat and associate adversary could perpetrate both medium and low level threats. However, the stealth nature of their exploits is determined by the properties of the victims, characteristics and the objectives as shown in the exploit confidence value of the association rule.

5. CONCLUSION

This work clearly demonstrates that threat could be rated from the perspective of attack exploits using Association Rules and Fuzzy Logic regardless of the imprecise knowledge of risk. Also, this paper proved the assertion that threat should be monitored in the inside and demilitarized zone of the network for reliable security. The paper considers attacks and attackers from a perspective different from previous works on intrusion prediction and prevention. It emphasizes that attacker’s change their exploits based on victim properties, their capabilities and objectives instead of either victim centric or attacker centric attack model. Moreover, the result conforms to what is reported about DARPA 2000 Scenario Dataset [7].

Nonetheless, this work focused on threats targeted at a single host with different characteristics of adversary. In future, we shall consider multiple hosts and use the result to predict intrusion.

REFERENCES

[1] Bhattacharya S., Ghosh S. K.2008. A Decision Model based Security Risk Management Approach. Proceedings of the International MultiConference of Engineers and Computer Scientists IMECS 2008, Hong Kong, Vol II, 19-21 March, 2008.

[2] Carlson, M. and Scharlott, S. 2006. “Intrusion Detection and Prevention Systems,” CS536 Final Paper May 05, 2006.

[3] Cheung. S, Lindqvist U., and Fong M. 2003. Modeling Multistep Cyber Attacks for Scenario Recognition. In Proceedings of the DARPA Information Survivability Conference and Exposition (DISCEX III), pages 284{292, Washington, D.C., April 2003.

[4] Dantu R., Kolan P., Akl R., Loper K. 2007. Classification of Attributes and Behaviour in Risk Management Using Bayesian Networks.1-4244-1330-3/2007 IEEE.

[5] Dondo M. 2007. Fuzzy Risk Calculations Approach for a Network Vulnerability Ranking System. Defence R &D Canada-Ottawa, Technical Memorandum DRDC Ottawa TM 2007-090 May, 2007, Pg 3.

[6] Haslum K., Abraham A. and Knapskog S. 2008. Fuzzy Online Risk Assessment for Distributed Intrusion Prediction and Prevention Systems Center for Quantifiable Quality of Service in Communication Systems Norwegian University of Science and Technology ,7491 Trondheim, Norway.

[7] http://www.ll.mit.edu/mission/communications/ist/corpora/ideval/data/index.html. Accessed May 10, 2012.

[8] http://web.nvd.nist.gov/view/vuln/ . Accessed July 13, 2012.

[9] Li Z., Lei J., Wang L., and Li D. 2007. A data mining approach to generating network attack graph for intrusion prediction. Fourth International Conference on Fuzzy Systems and Knowledge Discovery, 307-311.

[10] McHugh J., Christie A. and Allen J. 2001 Intrusion Detection1: Implementation and Operational Issues. CROSSTALK- The Journal of Defense Software Engineering, Software Engineering Institute, Computer Emergency Response Team/Coordination Centre.

[11] Mell P., Scarfone K. and Romanosky S. 2007. A Complete Guide to the Common Vulnerability Scoring System Version 2.0

[12] Poolsappasit N., Dewri R., and Ray I. 2012. “Dynamic Security Risk Management Using Bayesian Attack Graphs,” IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1.

[13] Salter C., Saydjari O.S., Schneier B. and Wallner J. 1998. Toward A Secure System Engineering Methodology.

[14] Sheyner O., Haines J., Jha S., Lippmann, R., and Wing, J. 2002. Automated generation and analysis of attack graphs. 2002 IEEE Symposium on Security and Privacy, Washington, DC, USA. 273.

[15] Witten I. H, Frank E.2000. Data Mining: Practical machine learning tools and techniques with Java implementations. Morgan Kaufmann, San Francisco, CA.