International Journal of Computing and Network Technology
ISSN (2210-1519)
Int. J. Com. Net. Tech. 5, No. 1 (Jan.-2017)

A STRIDE Model based Threat Modelling using Unified and-Or Fuzzy Operator for Computer Network Security

Salman A. Khan

Computer Engineering Department, University of Bahrain, Sakhir, Bahrain

Received: 31 Aug. 2016, Revised: 20 Dec. 2016 Accepted: 24 Dec. 2016, Published: (1 January 2017)

Abstract: In the present era, security has become a fundamental issue in efficient and proper functioning of computer and network systems. To prevent and mitigate a system, an important issue to understand how different threats could damage a network system. Keeping this issue under consideration, this paper proposes risk assessment and modeling of threats which shows the level of any attack. STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial of service, Elevation of privileges) is a model which covers numerous existing threats that are related to all security properties necessary for a secure network. An strategy has been proposed which takes the number and types of attacks as input and applies a fuzzy logic based threat assessment approach to assess the level of attack. The presented work uses a fuzzy operator, namely, unified AND–OR (UAO operator), and a decision-making approach based on a fuzzy rule.

Keywords: Network Security, Automated decision-making, Fuzzy logic, STRIDE.

1. INTRODUCTION

The word "security" means safeguarding against attack from an intruder (insider and outsider). Millions of dollars are lost worldwide due to network security breaches where different attacks affect network assets which are network hardware/software resources and information. The main purpose of security is to protect assets. Computer or network security strives to prevent and detect illegal and unauthorized use of a host (computer) or network. Thus, a secure network is the one that provides confidentiality, integrity, authentication, non-repudiation, and availability to all legitimate users [1]. A well-structured network follows a three-level security strategy [2]:

1. Prevention: Stop an attack from succeeding.
2. Detection: Detect and inform the administrator if the attack once takes place.
3. Mitigation: Ability to minimize the loss & recover from the attack.

Before developing a secure network, it is important to analyze the risk a network could be exposed to. That is, it is of utmost importance to know the level of damage an attack could cause to a system. The possible threats must be identified, and be determined as which aspect of security would be violated by a certain attack, prior to establishing a network. There are various ways to identify and prioritize threats. A process of recognizing, measuring, and investigating potential threats of a system is called Threat Modeling [3]. It involves identifying the possible threats and rating them based on their risk factors. Threat modeling is done to know the level of any attack (high, moderate, low etc.). Such levels can help in the mitigation strategies.

The selection of threat models is based on two distinct yet related factors. First is the description of security issues which the designer cares about. Second is based on security aspects, i.e. by just looking at a software or program one can easily define the set of possible attacks to categorize. This categorization of threats provide a systematic identification of threats in a structured manner. The above discussion gives the motivation to adopt STRIDE (Spoofing, Tampering, Repudiation, Information disclosure, Denial-of-service, Elevation of privileges) as the threat model due to its comprehensiveness. The STRIDE models was developed by Microsoft for categorizing threats [4]. The classification of threats in this model is done by categorizing the kind of exploit done by attacker or intruder. Furthermore, because it covers numerous attacks (see details in Section 2) and is a simpler yet comprehensive approach for threat identification, it's the best call to generate the threat level. Following the STRIDE model, starting from S and ending at E gives a

E-mail: engr.ahmeds@gmail.com

dense sense of direction as well as a definitive pattern to form a model which covers almost all the possible threats which may occur to a network or computer.

Threat	Definition	Example
Spoofing	Pretending to be someone else.	Ahmed pretending to be Khalid.
Tampering	Changing information	Modifying a packet as it goes over the network.
Repudiation	Denying an act	"I didn't login to your e-mail account"
Information Disclosure	Revealing information to unauthorized ones	Allowing a student to read other students grades and GPA etc.
Denial of Service	Damage service for other users	Blocking the internet access to legitimate user by sending numerous packets at once over the network
Elevation of Privilege	Having access while being unauthorized	Allowing a distant internet user to run commands is the example, but going from a limited user to admin is also EoP.

Figure 1. STRIDE threat definitions and examples

It is a noted fact that the STRIDE model, where each threat is unique in itself, cannot be analyzed using Aristotelian (logic based on the philosophy of the famous Aristotle) or binary logic. Therefore, a desperate requirement of an analytical approach arises that could integrate the complexity of such threats and construct tailored solutions [5]. Fuzzy Logic answers the call, since it has the potential of merging human knowledge into technical (computer based) decision making. In this work, fuzzy logic works in a way that crisp inputs are taken as the number of threats which outputs the level of attack.

The paper progresses with Section 2 presenting the detailed study of the STRIDE model. Section 3 provides a primer of fuzzy logic and its relationship to multi-criteria decision-making, Section 4 shows the proposed approach of synergizing fuzzy logic and STRIDE for threat detection. The results are discussed in Section 5, followed by conclusion in Section 6.

2. STRIDE MODEL

A potential violation of the security of a system or a network is a threat [6]. This may lead to loss of data, access to data by unauthorized person etc. which implies that certain criteria must be followed when developing a secure network. To counter different types of threats, modes of security has been divided into following five categories [7].

- Integrity - To assure that data has not been altered illegally
- Availability - Continuous presence of a service or resource
- Confidentiality - To safeguard information from revelation
- Authenticity - Ability to legalize a resource along with data
- Accountability - Skill to confidently relate specific incident to a particular entity

Considering the aforementioned issues, Microsoft introduced a model known as STRIDE which covers numerous and major network attacks. The term "STRIDE" is derived from an acronym for the following six threat categories [8] as given in Figure1.

The combination of threats (Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, and Elevation of privilege) in Figure 1 is referred to as the STRIDE model which is used for different issues related to network security such as identifying threats, dealing with threats and taking appropriate steps to prevent, detect, and mitigate various attacks.

Below, details of each threat in the STRIDE model are discussed, along with the various sub-threats under each threat.

A. Spoofing

Spoofing or "Identity spoofing" is a scenario in which a user X pretends to be a user Y by changing his identity or data and thus gains an illegal access to data. This may result in vulnerabilities, therefore it is necessary that the network needs to authenticate the user's identity. Therefore, spoofing can be eliminated through authentication property [9]. Below are the spoofing threats covered by STRIDE.

- URL spoofing – An erroneous/spoofed URL that directs to another website [10].
- MAC spoofing – Intruder changes its computer's MAC address [11].
- Email spoofing – A spoofed email is sent using the email address of trusted user [12].
- DNS spoofing – Data is sent into a (DNS) server's cache database, returning wrong IP address and thus diverting traffic to hacker's computer [10].
- ARP spoofing – Spoofed Address Resolution Protocol is created which diverts the traffic to hacker's computer [13].

- IP spoofing – Attacker sends data using a trusted users IP address [10].

B. Tampering

As the name implies, tampering refers to change of data by an illegal person who is not authorized to modify it. If packets sent by a user over a network are tampered, it would result in affecting the integrity of the system [4]. Thus, the integrity can be maintained by blocking an unaccredited user from manipulating the data. The system needs to examine data received from any user and confirm that the message received by the user has not been altered. Tampering is handled by STRIDE with respect to the following:

- Spyware – Software gathers information about a person/company without telling it [14].
- Crimeware – Software that commits crime over internet [15].
- Trojan horses – Malware causing loss of data or damages the system [10].
- Relay attacks – Illegal modification of data which user is not able to doubt [10].

C. Repudiation

This category relies on the fact that a security system must always be able to trace the entity responsible for any illegitimate modification and illegal access of resource or account. This is known as the non-repudiating act of any network. In contrast, repudiation is the situation where any user does not agree on performing an act and is not able to identify the one who did this illegally, such as sending an email, transaction of money etc. Due to these reasons there is a need of auditing and keeping record of all the activities over a network [16]. Users may dispute transactions if there is insufficiency in these needs. This falls under the property of accountability. Thus, repudiation takes care of the fact that the user cannot deny after performing an act [9]. STRIDE takes care of the "masquerading attack" where intruder gains illegal access to personal data through a valid user's identification using fake identity [17].

D. Information Disclosure

Information disclosure assists an attacker or malicious user in achieving confidential information for which he is not permitted. Users are fairly cautious of submitting private details to a system or other user through network. Personal details, bank account details or business details are meant to be confidential for the users which mean that only the intended person should be able to see and utilize that data [18]. To safeguard such sensitive data from leakage, the confidentiality of data must be maintained [4]. STRIDE is capable to responding to the following types of information disclosure.

- Phishing – Using a valid user's identity, intruder gains username, password etc. [10].
- Sniffing – Attacker observes the data flow through the network links [19].
- Man-in-the-middle – Attacker being a middle man changes the messages between the sender and the receiver before the receiver reads the message [15].
- Compromised-key - Hacker determines the key which he uses to decrypt the encrypted data without informing the sender [20].
- Path Traversal – "Access files and directories that are stored outside the web root folder." [10]
- Predictable Resource Location – Intruder uses this skill to reveal hidden website content [19].
- Ransom ware - Malware that constrains valid user to access to his files [10].
- WiFi Eavesdropping -Virtually listens to personal information such as logins and passwords [7].

E. Denial of Service

Denial-of-service (DoS) attack is an attempt to disturb a resource, network, or system in such a way that the intended and valid user wouldn't be able to use it. The attackers usually do this through blocking the network by sending infinite packets over the network [21]. This blocking can be done at the destination, communication channel or by discarding messages between sender and receiver. In order to prevent such attacks the network security is responsible to ensure that the system or resource is always available to the valid users. Following DoS attack types are handled by STRIDE.

- UDP bombing – Floods the receiver with numerous UDP packets [10].
- TCP SYN flooding – During the process of three way hand shaking, the intruder floods the victim server with several SYN packets with spoofed IP addresses. Due to long queue, all succeeding SYN requests are ignored, therefore no TCP sessions takes place [9].
- Ping of death - Attacker generates an IP packet that is more than 65,536 causing the victim's system to crash, hang, or reboot [15].
- Smurf attack – Knowing the IP and ICMP of the target, the network is made inoperable [10].

- Teardrop attacks- IP fragments with overlapping and over-sized payloads are sent to the victim's system which may crack it [4].
- Slow Read attack – Sends valid application layer requests but responses are read slowly, which exhaust the server's connection [16].
- Slowloris - software which keeps various connections open to the victim's web server and hold them open till possible [10].
- R-u-Dead-Yet (RUDY) - Goals web applications by starvation of available sessions on the web [19].
- Snooping – Intruder observes the email content or what the user is typing [10].

F. Elevation of Privilege

Elevation of privilege is the category of attacks in which the intruder gets the authorization more than what has been granted originally. This means that any user is not admitted to elevate his privilege to a higher level on his own. Concerning the authorization property of network security, it is very important to guarantee that solitary the legalized roles can access restricted functionality [9].

- All the above discussion can be tabulated as following [8]. STRIDE takes care of the following issues in this category.
- Adware – Advertisements are shown while the program is debugging [17].
- Worms – Malware that repeats itself to spread to other PCs [10].
- Luring attack – A highly privileged component is convinced to do something on its behalf [20].

3. Fuzzy Logic and Multi-criteria Decision Making

The ideas of fuzzy logic were initially proposed by Zadeh in 1965 [22]. Despite initial resistance by the research community who considered the theory of fuzzy logic controversial, the logic has received tremendous attention in the last four decades, and its applications have increased significantly. Till date, fuzzy logic has been applied to a diverse areas, from control theories to artificial intelligence [23], with applications such as analog circuit design [24], war resource allocation [25], direct current electromagnet design [26], and facility location selection [27], among many others.

One major application of fuzzy logic is in the area of multi-criteria decision making (MCDM). Multiple criteria decision making (MCDM) is a technique used in scenarios where decisions need to be made in presence of multiple and conflicting criteria. MCDM is concerned with decisions about selecting the best alternative from a finite set of available alternatives. The presence of multiple criteria triggers a number of issues involved with MCDM. In majority of problems, the data associated with criteria are non-commensurate. A number of approaches such as goal programming and weighted aggregation exist to deal with this issue, fuzzy logic has also been effectively used to solve a number of MCDM problems involving this issue. Another primary reason to consider fuzzy logic for MCDM problems is the approach fuzzy logic handles uncertainties in design data. Although it is possible to describe uncertainties in terms of conditional probabilities, it is difficult in the majority of practical cases. A framework for representing such knowledge is easily provided by fuzzy logic.

In dealing with MCDM problems using fuzzy logic, criteria are combined to form an overall decision function which is scalar value. An important concern is the selection of an appropriate function, since there are wide variety of fuzzy functions available. Usually, the objective in MCDM problems is to satisfy all criteria simultaneously, resulting in the "pure ANDing" operation. However, the pure ANDing operation is traditionally represented as the "Min" function, as defined by Zadeh. In mathematical terms, this representation is very rigid, since it only considers the effect of the lower quality criteria, while completely ignoring the positive effect of the higher quality criteria. This observation led to the development of soft-And and soft-Or operators.

The Unified And-Or (UAO) operator, proposed by Khan and Engelbrecht [28], is a soft-And and soft-Or operator at the same time. The key feature of the operator is that a single equation is used to represent the soft-AND function or the soft-OR function. The behavior of the operator is controlled by a variable $\nu \geq 0$, whose value decides whether the function behaves as soft-AND or soft-OR. The operator is defined as

$$f(a,b)=\frac{ab+\nu\max\{a,b\}}{\nu+\max\{a,b\}}=\begin{cases}\mathrm{I}_{*}=\mu_{A\cup B}(x) & \text{if } \nu>1\\ \mathrm{I}^{*}=\mu_{A\cap B}(x) & \text{if } \nu<1\end{cases}$$

where 'a' represents the membership value of first decision criteria, 'b' represents the membership value for second decision criteria and f(a, b) represents the value of the overall objective. I^* represents the soft-AND operation using the UAO operator, and I_* denotes the soft-OR operation using the UAO operator. With $0 < \nu < 1$, the behavior of UAO is soft-AND, whereas a value of $\nu = 0$ gives the pure-AND behavior of Zadeh's MIN function. Further details and mathematical properties of the UAO operator are given in [28].

4. Fuzzy Logic based Multi-criteria STIRDE Threat Detection Approach

Threat detection with STIRDE requires a multi-dimensional strategy due to the huge variety of attacks to be dealt with. This motivates the need of having a detection scheme that would be capable of dealing with all threats covered by STRIDE. In other words, the scheme should be able to handle all six categories of threats. This signifies that the STRIDE threat detection scheme can be formulated as a multi-criteria decision-making scheme. The function of such a threat detection system would be to identify a single attack or stream of attacks on the network, where the system would raise an alarm based on the intensity and type of attack.

The proposed system would require four main steps, as enumerated below.

1. Fuzzifying each threat by defining its fuzzy membership function
2. Aggregating each fuzzified threat into a single decision function
3. Depending on the designer, give preference of one or more threats over the other(s)
4. Interpreting the results of the Step 2 and Step 3 and taking necessary action accordingly.

Each step of the proposed strategy is explained below.

A. Fuzzification of the threats

In this step, each of the six threats are fuzzified. This requires mapping the actual number of attacks into a fuzzy membership range. To define a membership function, the upper and lower bounds for each threat type are needed. Based on the available literature [3][19][20][21], the following ranges have been proposed for each threat type .

Spoofing - (0 – 10)

Tampering – (0 – 25)

Repudiation – (0 – 15)

Information Disclosure – (0 – 30)

Denial of Service – (0 – 40)

Elevation of privilege – (0 – 5)

The membership functions are defined as follows. Note that linear representations are used to define each membership function.

The membership function for Spoofing is formed by using the two extreme values (upper and lower bounds) . The two limits, SMin and SMax, are as mentioned above (0 and 10 respectively). The membership function for Spoofing, $\mu_S(x)$, is mathematically represented as follows.

$$\mu_S(x) = \begin{cases} 1 & \text{if } Spoofing(x) \geq SMax \\ \frac{Spoofing(x)-SMin}{SMax-SMin} & \text{if } SMin \leq Spoofing(x) < SMax \\ 0 & \text{if } Spoofing(x) < SMin \end{cases} \quad (1)$$

The membership function for Tampering is formed by using the upper and lower bounds which are TMax and TMin respectively. The membership function for Tampering, $\mu_T(x)$, is mathematically represented as follows.

$$\boldsymbol{\mu_E(x)} = \begin{cases} 1 & if\ Tampering(x) \geq TMax \\ \frac{Tampering(x)-TMin}{TMax-TMin} & if\ TMin \leq Tampering(x) < TMax \\ 0 & if\ Tampering(x) < TMin \end{cases} \quad (2)$$

Similarly, the membership function for Repudiation can be formed as follows. The two bounds for repudiation are determined first, using the collected data. Equation (3) represents the membership function, $\mu_R(x)$, for Repudiation. In this equation, RMax =15 and RMin = 0 correspond to the upper and lower bounds, respectively.

$$\mu_R(x) = \begin{cases} 1 & if\ Repudiation(x) \geq RMax \\ \frac{Repudiation(x)-RMin}{RMax-RMin} & if\ RMin \leq Repudiation(x) < RMax \\ 0 & if\ Repudiation(x) < RMin \end{cases} \quad (3)$$

The membership function for Information Disclosure can be formed in the same manner. The upper and lower bounds are taken from the data range where the upper limit IMax = 30 and IMin = 0. The membership function $\mu_I(x)$ will be as follows.

$$\mu_R(x) = \begin{cases} 1 & if\ InfoDisc(x) \geq IMax \\ \frac{InfoDisc(x)-IMin}{IMax-IMin} & if\ IMin \leq InfoDisc(x) < IMax \\ 0 & if\ InfoDisc(x) < IMin \end{cases} \quad (4)$$

With respect to the membership function for Denial of Service, the upper bound DMax = 40 and the lower bound DMin = 0. The membership function $\mu_D(x)$, is defined as given in Equation (5).

$$\mu_D(x) = \begin{cases} 1 & \text{if } DoS(x) \geq DMax \\ \frac{DoS(x)-DMin}{DMax-DMin} & \text{if } DMin \leq DoS(x) < DMax \\ 0 & \text{if } DoS(x) < DMin \end{cases} \quad (5)$$

Finally, Elevation of Privileges can have a membership function as given in Equation (6). In this equation, upper limit EMax = 5 and lower limit EMin = 0.

$$\mu_E(x) = \begin{cases} 1 & \text{if } EoP(x) \geq EMax \\ \frac{EoP(x)-EMin}{EMax-EMin} & \text{if } EMin \leq EoP(x) < EMax \\ 0 & \text{if } EoP(x) < EMin \end{cases} \quad (6)$$

B. Aggregation of membership function

After all membership functions are found, the next step is to aggregate all into one decision function. This decision function can be stated as fuzzy rule as follows:

Rule 1: "IF spoofing is low AND tampering is low AND repudiation is low AND information disclosure is low AND denial of service is low AND elevation of privilege is low then the attack is low"

The above rule indicates the conditions which would classify the level of attack. The above rule can be implemented as a t-norm in mathematical terms using the UAO operator as follows

$$f(x) = \frac{\mu_S \mu_T \mu_R \mu_I \mu_D \mu_E + \nu.\max\{\mu_S, \mu_T, \mu_R, \mu_I, \mu_D, \mu_E\}}{\nu + \max\{\mu_S, \mu_T, \mu_R, \mu_I, \mu_D, \mu_E\}} \quad (7)$$

In the above equation, f(x) represents the overall decision function. This overall decision function signifies the level of attack on the network. Note that the value of f(x) is in the range of [0,1]. The nearer the value of f(x) to 1, the higher is the level of attack, whereas a low value of f(x) indicates a low level of attack.

C. Interpretation of decision rule

The final step is the generation of the threat levels based on the threat rule. For the sake of this paper, three parameters are defined to detect threat level i.e. 'Low', 'Moderate' and 'High'. Again, these levels and their corresponding ranges are flexible and can be adjusted by the security administrator as desired.

Recall that f(x) represents the output of the UAO operator. Thus, the ranges are defined as follows.

For $0 < f(x) < 0.3$ the threat level is 'Low'

For $0.3 < f(x) < 0.5$ the threat level is 'Moderate'

For $f(x) > 0.5$ the threat level is 'High'

5. Results and Discussion

The proposed system was tested on hypothetical data consisting of various types of attacks. 20 instances were considered where the nature and level of attacks were varied. Table 2 defines the actual frequency and types of these attacks. Moreover, Table I provides the corresponding individual membership function for each attack type, the aggregated UAO value, and the level of attack as discussed below

Table II provides the membership values for each individual attack type corresponding to the intensity of the attack. As observed in the table, the attacks are either moderate or low. One interesting observations from the above table is that there are several attacks that are in the moderate category having the same overall impact. As a case, consider attacks 5, 8, 12, and 15 are all having the same intensity signified by the f(x) value of 0.308, but their nature is totally different:

Attack 5: Repudiation = 6, Denial of Service = 26, and Elevation of Privilege = 4

Attack 8: Spoofing = 8, Information disclosure = 24, and Elevation of Privilege = 3

Attack 12: Tampering = 20, Repudiation = 7

Attack 15: Tampering = 20, Denial of Service =29

The above scneairo indicates that the system would assess the overall impact of the attack as measured by the fuzzy logic based unified and-or function given in Equation (7) according to Rule 1 . This overall impact is based on the impact of individual attacks for the data given in Table I.

TABLE I. ATTACKS TYPES AND FREQUENCIES OF ATTACKS FOR 20 DIFFERENT ATTACKS.

Attack	S (0 - 10)	T (0 - 25)	R (0 - 15)	I (0 - 30)	D (0 - 40)	E (0 - 5)
Attack 1	7	0	0	20	0	0
Attack 2	0	22	8	0	0	2
Attack 3	0	17	0	0	17	0
Attack 4	5	0	0	19	0	0
Attack 5	0	0	6	0	26	4
Attack 6	0	0	15	0	38	0
Attack 7	0	19	0	17	0	0
Attack 8	8	0	0	24	0	3
Attack 9	4	0	0	0	35	0
Attack 10	0	0	0	0	0	2
Attack 11	0	0	9	0	27	0
Attack 12	0	20	7	0	0	0
Attack 13	3	0	0	26	34	0
Attack 14	10	0	0	0	25	0
Attack 15	0	20	0	0	29	0
Attack 16	0	19	0	0	0	0
Attack 17	3	0	0	27	0	3

Attack 18	0	0	14	0	0	1
Attack 19	0	18	0	0	34	0
Attack 20	4	0	7	0	0	0

6. CONCLUSION

This work proposed a threat modeling scheme by applying fuzzy logic based approach to the STRIDE threat model. The crisp numbers signifying the number of attacks on a network systems were given as input. These numbers of attacks were fuzzified and then evaluated using the unified and-or fuzzy operator. The result then led us to decide the level of attack. Preliminary empirical analysis indicate that the proposed approach satisfactorily addresses the issues of measuring impact of several simultaneous attacks. Future work will focus on the application of other techniques mentioned earlier (such as goal programming and weighted aggregation) to the underlying problem, as well studying the impact of criteria preference on the problem addressed in this paper.

Acknowledgment

The author thanks the Deanship of Scientific Research at University of Bahrain for supporting this work under Project # 24/2015. The author also acknowledges the assistance provided by Mr. Faiz Iqbal.

TABLE II. MEMBERSHIP VALUES OF ATTACKS AND OVERALL LEVEL. H = HIGH, M= MODERATE, L = LOW.

Attacks	μ_S	μ_T	μ_R	μ_T	μ_D	μ_E	f(x)	Level
Attack 1	0.70	0.00	0.00	0.67	0.00	0.00	0.292	L
Attack 2	0.00	0.88	0.53	0.00	0.00	0.40	0.319	M
Attack 3	0.00	0.68	0.00	0.00	0.43	0.00	0.288	L
Attack 4	0.50	0.00	0.00	0.63	0.00	0.00	0.279	L
Attack 5	0.00	0.00	0.40	0.00	0.65	0.80	0.308	M
Attack 6	0.00	0.00	1.00	0.00	0.95	0.00	0.333	M
Attack 7	0.00	0.76	0.00	0.57	0.00	0.00	0.302	M
Attack 8	0.80	0.00	0.00	0.80	0.00	0.60	0.308	M
Attack 9	0.40	0.00	0.00	0.00	0.88	0.00	0.318	M
Attack 10	0.00	0.00	0.00	0.00	0.00	0.40	0.222	L
Attack 11	0.00	0.00	0.60	0.00	0.68	0.00	0.287	L
Attack 12	0.00	0.80	0.47	0.00	0.00	0.00	0.308	M
Attack 13	0.30	0.00	0.00	0.87	0.85	0.00	0.317	M
Attack 14	1.00	0.00	0.80	0.00	0.63	0.00	0.333	M
Attack 15	0.00	0.80	0.00	0.00	0.73	0.00	0.308	M
Attack 16	0.00	0.76	0.00	0.00	0.00	0.00	0.302	M
Attack 17	0.30	0.00	0.00	0.90	0.00	0.60	0.321	M
Attack 18	0.00	0.00	0.93	0.00	0.00	0.20	0.326	M
Attack 19	0.00	0.72	0.00	0.00	0.85	0.00	0.315	M
Attack 20	0.40	0.00	0.47	0.00	0.00	0.00	0.241	L

REFERENCES

[1] The STRIDE Threat Model, http://msdn.microsoft.com/enus/library/ee823878%28v=cs.20%29.aspx, 2002

[2] M. Curtin, Introduction to Network Security, Kent Information Services, Inc., March 1997.

[3] A. S. Sodiya, S. A. Onashoga and B. A. Oladunjoye, Threat Modeling using Fuzzy Logic Paradigm, Volume 4, 2007

[4] A. Shostack, S. Lambert, S. Hernan, Uncover Security Design Flaws using STRIDE, MSDN magazine, November 2006.

[5] S. S. Godil, M. S. Shamim, Fuzzy logic: A “simple” solution for complexities in neurosciences?, http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3050069/

[6] C. Wijayayunga, Internet and Network Security Fundamentals, pg. 10-20, 1990

[7] W. Stalling, L. Brown, Computer Security: Principles and Practice, 2nd edition, Pearson Education, 2008.

[8] B. Daya, Network Security: History, Importance, and Future, University of Florida.

[9] M. A. Anton, J. M. Barnes, STRIDE-based Security model, Institute of software research, January 2010.

[10] Common Threats, http://www.getcybersafe.gc.ca/cnt/rsks/cmmn-thrts-eng.aspx, Feb 2014

[11] Al-Salqan, IT Security Trends, http://www.sophos.com/en-us/security-news-trends/security-trends/network-security-top-trends.aspx, distributed computing systems, 1997.

[12] G. Oltean, C Miron, and E. Moccan. Multiobjective Optimization for Analog Circuits Design based on Fuzzy Logic. In 9th International Conference on Electronics, Circuits and Systems, pages 777 – 780, 2002.

[13] L. A. Zadeh. Fuzzy Sets. Information Control, 8:338–353, 1965.

[14] S. Pandey, Modern Network Security: Issues and Challenges, IJEST, Vol. 3, May 2011.

[15] ASA Threat Detection Functionality and Configuration, http://www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html, Accessed December 2015.

[16] B. Floyd, The Changing Face of Network Security Threats, IEEE, SCTE, May 2006.

[17] J. E. Canavan, Fundamentals of Network Security, Artech House telecommunications library, 1999.

[18] Adeyinka, O., Internet Attack Methods and Internet Security Technology, Modeling and Simulation, 2008. AICMS 08. Second Asia International Conference on, pg. 77-72, Nov 2005.

[19] A. Ahmad, Type of security Threats and it's Prevention, Int.J.Computer Technology & Applications, Vol 3(2), 750-752, 2012.

[20] Threat in an Enterprise Network, Designing Network Security, 2nd Edition, 2009

[21] Ohta, T.; Chikaraishi, T., Network Security Model, http://www.sans.org/reading-room/whitepapers/modeling/network-security-model-32843, Accessed Jan. 2016.

[22] J. Kacprzyk, M. Fedrizzi, H. Nurmi, Group decision making and consensus under fuzzy preferences and fuzzy majority, Fuzzy Sets and Systems 49, 21–31, 1992.

[23] J. Kacprzyk, Group decision making with a fuzzy linguistic majority, Fuzzy Sets and Systems 11,105–118. 1996

[24] G. Oltean, C Miron, and E. Moccan. Multiobjective Optimization for Analog Circuits Design based on Fuzzy Logic. In 9th International Conference on Electronics, Circuits and Systems, pages 777 – 780, 2002.

[25] S. Palaniappan, S. Zein-Sabatto, and A. Sekmen. Dynamic Multiobjective Optimization of War Resource Allocation using Adaptive Genetic Algorithms. In IEEE SoutheastCon, pages 160 – 165, 2001.

[26] M. Chiampi, C. Ragusa, and M. Repetto. Fuzzy Approach for Multiobjective Optimization in Magnetics. IEEE Transactions on Magnetics, 32(3):1234 – 1237, 1996.

[27] C. Kahraman, D. Ruan, and I. Doan. Fuzzy Group Decision-making for Facility Location Selection. Information Sciences, 157:135–153, 2003.

[28] S. A. Khan and A. P. Engelbrecht. A new fuzzy operator and its application to topology design of distributed local area networks. Information Sciences, 177(13), pp.2692-2711, 2007.

Salman A. Khan received M.S. in Computer Engineering from King Fahd University of Petroleum & Minerals, Saudi Arabia in 2000 and the PhD degree in Computer Science from University of Pretoria, South Africa in 2009. He is currently an Assistant Professor in the Computer Engineering Dept. at University of Bahrain, and an Adjunct Senior Researcher with Computational Intelligence Research Group, Computer Science Department, University of Pretoria. He has published over 30 research articles in reputed journals and conferences. His research interests include Evolutionary Computation, Swarm Intelligence, Nature-inspired Algorithms, Fuzzy Logic, Single-objective and Multi-objective optimization and decision-making, Computer Networks, and Mobile Communication Systems. He serves as a reviewer for various reputed journals and conferences annually