Vol. 5(17) Oct. 2015, PP. 2500-2506

Contents list available at IJMEC

International Journal of Mechatronics, Electrical and Computer Technology (IJMEC)

Journal Homepage: www.aeuso.org

PISSN: 2411-6173 - EISSN: 2305-0543

Increasing the Security of Site Manager's Password Using Fuzzy Inference System

Raheleh Shariatpanahi[1*] and Nasser Modiri[2]

[1]*Department of Computer, Zanjan Branch, Islamic Azad University, Zanjan, Iran*

[2]*Department of Computer, Zanjan Branch, Islamic Azad University, Zanjan, Iran*

***Corresponding Author's E-mail:** Rahele_shariatpanahi@yahoo.com*

Abstract

According to some researches one of the commonest methods of hacking and copying the information of organizations is, weak passwords. By reviewing the literature we found out nobody has used fuzzy inference system yet, so we preferred to create one fuzzy inference system. It can increase the security of password by standards that we have decided for it. Our method shows the security to site's manager so that he can update his password to choose the best code. For analyzing our method, we compare it with the system logs.

Keywords: *Insider threat, Password, site's manager, Cyberspace.*

1. Introduction

One of the most important facts in organizations is the security of cyberspace of their networks, since fighting with treat groups is very difficult and there is no end to their threats. One of the commonest methods of hacking and copying the information of an organization is because of using weak passwords that site's manager has used. So site's manager should put an emphasis on the security of passwords to prevent misusing of resources and so on [1]. In our study, we have emphasized on increasing the security of Site Manager's Password. We have used a fuzzy inference system because by its logic it can help us to achieve our goal-showing the best password. In fact, this mechanism enables the site's manager to get and update the password with the lowest expense. Here we should same points about fuzzy logic. Theory of fuzzy sets is used to express and explain lack of certainty and accuracy in events and basic key of fuzzy theory is created by multipurpose logic. Fuzzy theory supports impossible lack of certainty. In fact, it develops the concept of zero and one and binary of theory of classic sets and proposes the rated membership, so that an element can be a member of a set not completely. In this theory the membership is specify by function of u(x), that x is a specific member and u is a fuzzy function that determine the rate of membership of x and it quantity is between zero and one.

$$\tilde{A} = \{(x, \mu_A(x)) \mid x \in X\} \quad (1)$$

Fu(x) maybe a set of discrete or continuous values, in other words u maybe some of the discrete values between zero and one-for example 0.3, 0.5, 0, 1 or it may be continuous that make a continuous curve of decimal numbers between zero and one. So, to achieve the best password we created a fuzzy inference system based on some rules and it heart is a database which is based on if - then fuzzy rule, one of our rule is:

$$if\ (input\ link\ is\ bad)\ and\ (web\ alert\ is\ bad)\ then\ (password\ is\ V\ Good) \quad (2)$$

Article History:

Received Date: Jun. 06, 2015

Accepted Date: Sep. 04, 2015

Available Online: Sep. 19, 2015

To design the system there are many different function of membership but we used Triangular Membership Function. There is a sample in Figure 1.

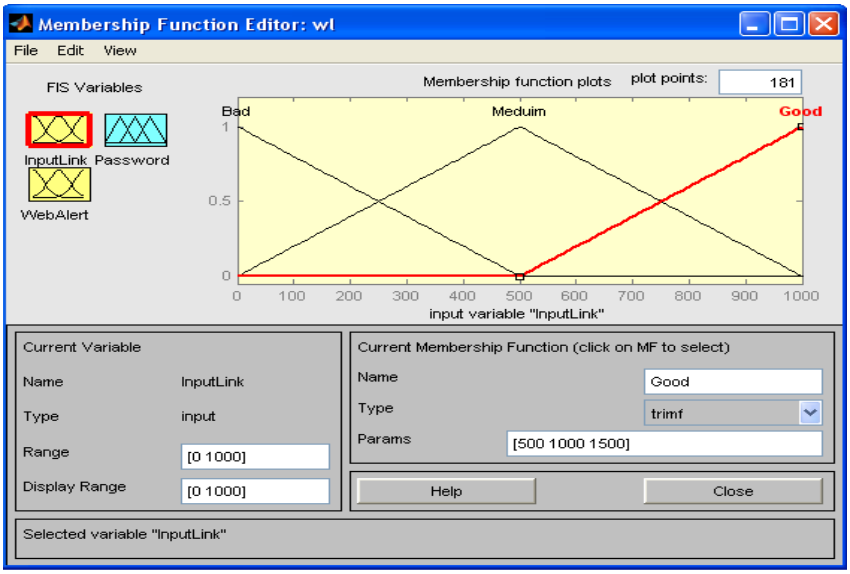

Figure1: Example of membership functions

Due to the important of the subject so many works have been done. Here we review some of these works. In an article the writer has studied the way of identification of risks of cheating and developed the all parts of cheating in the administrator program of managing risks successfully [2]. Another article, "Information on security National union of cyber council", explains the insider threats of workers [3].

"What is the Insider Threat?" is an article has been done by (TSC) company. This company is creative in security of staffs. It suggests that the best training in security is a level that decreases the risks and improves the business [4].

An article focuses on providing security and defends of governmental cyber system and manages different ways of threats and Vulnerability of cyber systems [5]. Another article studied the metrics of cyber security and its goals. This metrics can control the security and find its strong and weak points [6].

There is a thesis that focuses on finding the characteristics of the flow of information and suggests a model for it in CPSs [7]. Analyzing the flow of secured information in physical cyber systems is the subject of an article based on CPS [8]. Because of the fast growth of internet crime and other net threats we should know some important points about its risks and to protect what has become a part of our economics and society we should work and help each other [9].

Reporting intellectual property crime it's a guide for victims of copyright infringement, trademark counterfeiting, and trade secret theft [10]. The rise of financial fraud, a primary goal of this report is to provide insight into the disguises con men use to perpetrate their standard fraud schemes and to recruit victims who may be retirees, members of the military, college students, the unemployed, homebuyers, investors, low-income families, and others [11]. Internet crime 2012 studies the monthly reports, public services news, warning about frauds and online crimes [12]. Internet scam guide, The Internet is becoming a big part of our everyday lives. But there are no gatekeepers on the "information superhighway." New, unregulated technology means new opportunities for consumers, investors, businesses and for scam artists [13].

"How we can be away from deceit?" is a book about all things about internet fraud [14].

Engineering of the security of networks of computer is the subject of a book about how we can choose a secured password [15].

2. Suggested Work

2.1. Software used

For increasing the security of Site Manager's password we have used fuzzy system in MATLAB. We have done it based on fuzzy theory because it has been useful. So far, this logic view the world not based on facts of zero and one but based on a gray spectrum of facts. So to get good result we used fuzzy. It help the site's manager to enter the password in cyberspace and then based on fuzzy inference system analyzing the password is done and by defined standards in our system, searching and choosing in final database is done and then, after some computations suitable password as an output will be produced.

The inputs of our system are 1) the number of input links of each site that have been introduced by other sites 2) the number of web alerts that has been gained by testing the security of the site. The output of the system is the password of the site's manager that after some inner computations has been done and then the security of the password according to criteria of the site has been recorded as an output.

3. Modeling and Evaluation

3.1. Procedure

A summary of work has been shown in Figure 2.

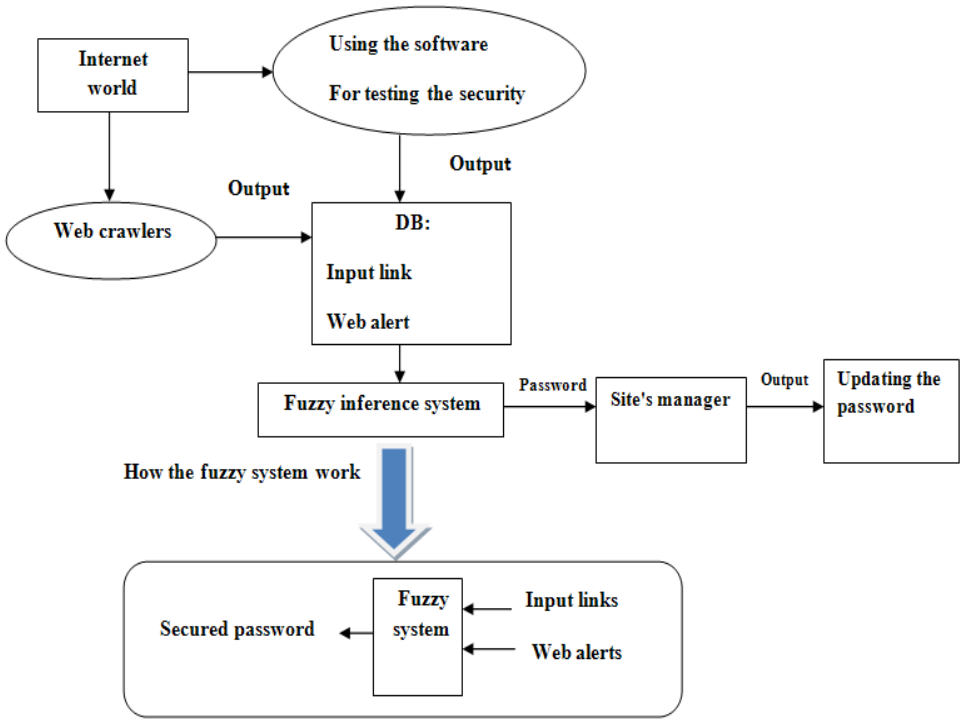

Figure2: Description of work

3.1.1. Web crawler: To have good data base the first and best step is using web crawler to find the number of the input links.

3.1.2. Site security testing software: After recognizing three security testing software, ACUNETIX Web Vulnerability Scanner, NETSPARKER, Shadow Security Scanner that make the bugs and web alerts known for us and also by using web crawler, 80leges.com(online) and web content extractor (offline) we get and find the input links and came to this results:

1) More input link, more famous the site and more viewing the site So more activity of hackers.
2) More bugs and web alerts, more risk of hacking.

3.1.3. Database: Our database is the result of the output of web crawler and security testing software.

3.1.4. Site's manager: Based on the rules of fuzzy inference system, Site's manager to prevent misusing the password should update and control the password.

3.2. Fuzzy inference system

This system is the basic part of our suggested work. It has been already said that it has two inputs and one output that will be explained below.

The first input is the input links it is among (0-1000), the worst case is zero and the best in 1000. If it be more, it will be better. To define these variables we have decided a range of more or less for their starts and ends, it means the amount of "1000" is good. More input links, more famous the site.

Another input is the number of web alerts it shows that there is more risks that threat our site. There is a range of (0-40) for this part. The zero is the best condition and the 40 is the worst.

After these two inputs perform their computation they will have a result that generates an output, the secured password, it is between (0-50). A password is call good which it hasn't less then 10 characters. 50 characters is the best, these standards together can be a good criterion for our site. Both of them are preformed on a small database and we come to a good result, it is clear that getting good result means that it can be on other big databases too.

3.3. Determining the rules

In fuzzy system to do the works, there must be some rules. They should be chosen carefully. Here we have approximately 40 rules and we have defined for them some functions that determining goodness or badness of the standards. Figure 3 shows a curve of the established rules; more input links, more secured password. It means when our input links are great in numbers, the password must be stronger.

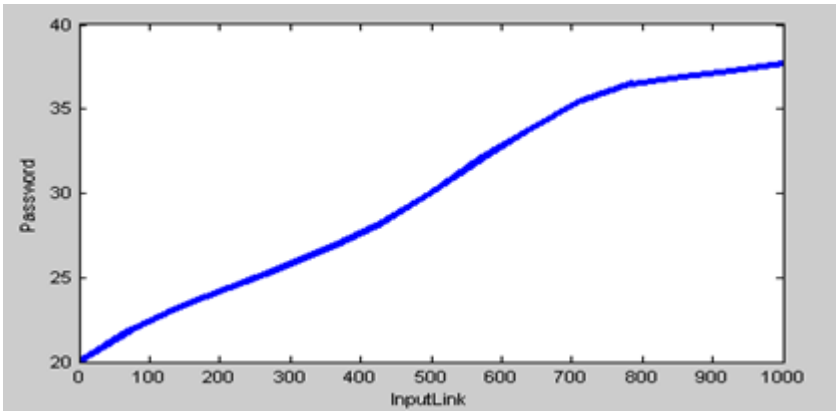

Figure3: A two dimensional diagram with input links input

Figure 4 shows the input web alerts. If the web alerts are great in numbers, the password must be stronger.

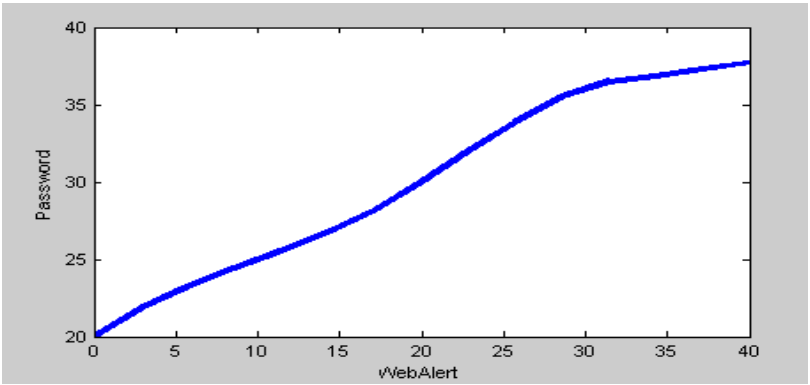

Figure4: A two dimensional diagram with web alert input

Finally, when the inputs were generated, the characteristics of the site will entered in the system and after evaluating it according to the determined rules the output will be the password.

4. Comparison and Testing

We tested the security of each site using ACUNETIX Web Vulnerability Scanner, NETSPARKER, Shadow Security Scanner, and for each site we show an output separately. There is an example for in figure 5.

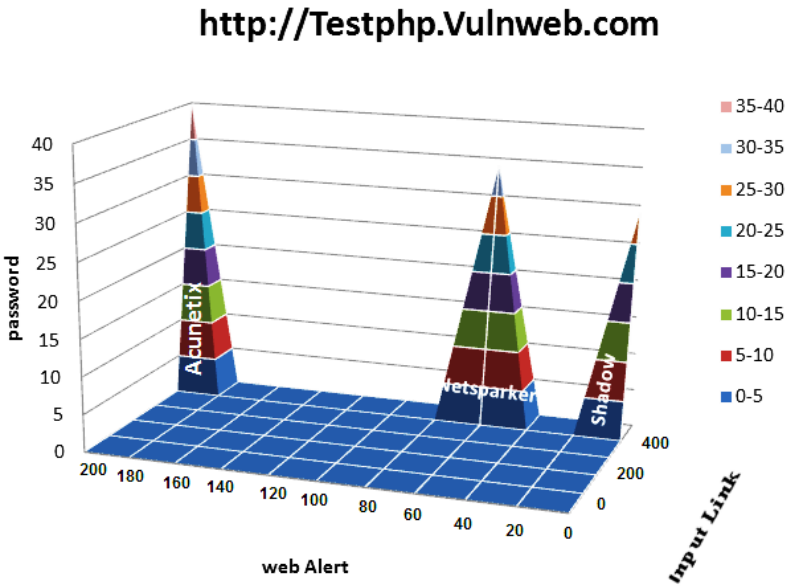

Figure5: Administrator password http://testphp.vulnuweb.com

Table1 shows the results.

Table1: Compare password in between three security testing software

Shadow Security Scanner	NETSPARKER	ACUNETIX Web Vulnerability Scanner	Software / Features
465	465	465	the number of input links
20	44	187	the number of web alerts
medium	Important	medium	Level of web alert
medium	Good	Very Good	Password in fuzzy system

After testing http://testphp.vulnuweb.com we found out it is easy to hack it. So the site's manager must update the password and increase the security of the site it means that his password must have at least 40 characters. Finally, we have done a comparison by system logs. Our use of this mechanism is 70 percent [16]. Figure 6 evaluate 10 sites that by increasing the level of the security of the password we have decreased the system logs mechanism.

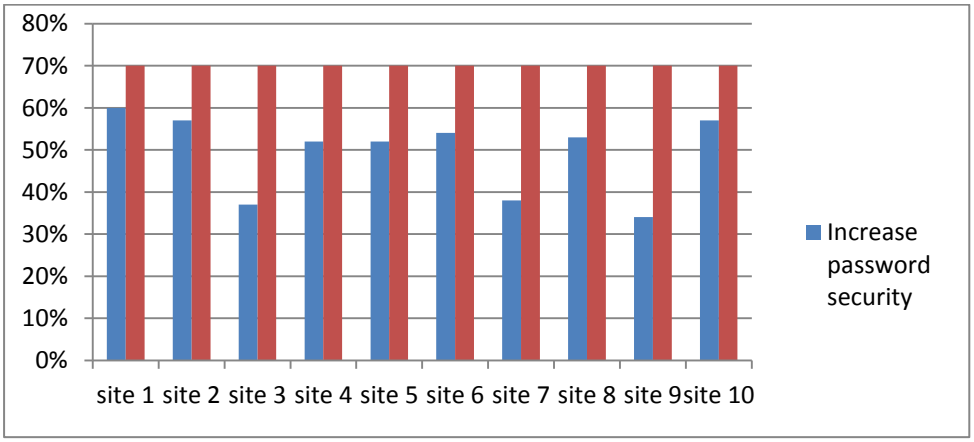

Figure6: Chart of the decrease the system logs mechanism using of fuzzy

Figure 7 shows the decrease in system logs index that compare 3 Indices among 10 sites; remote access logs, file access logs, system file change logs.

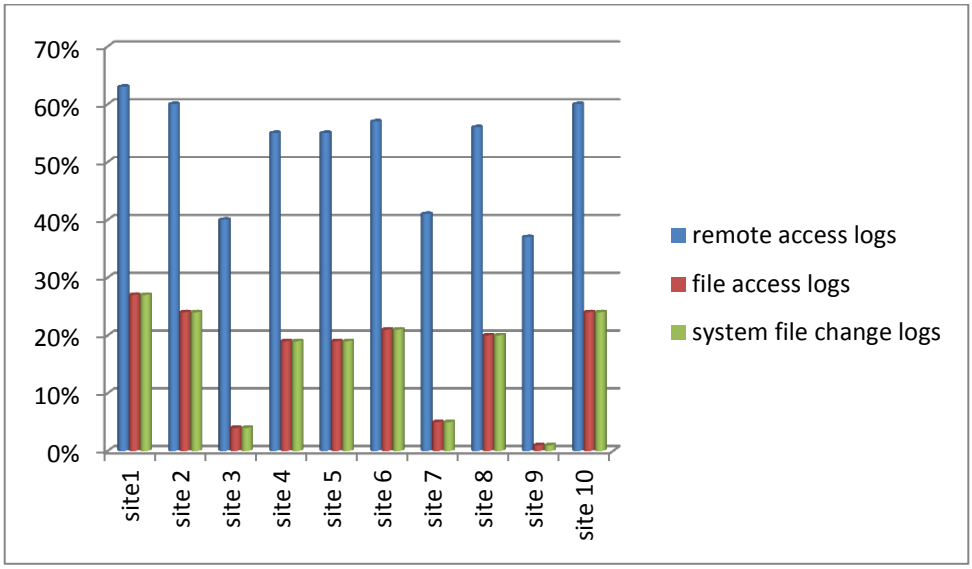

Figure7: Chart of the decrease in system logs Indices using of fuzzy

Figure 8 show the average of the result of 30 sites in decreasing system logs mechanism.

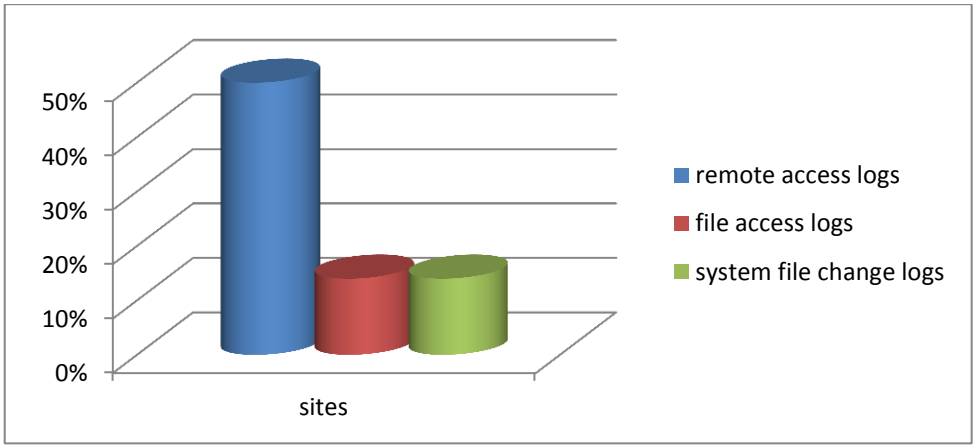

Figure8: Chart of the average of the result of 30 sites

Conclusion

Since one of the commonest ways for hacking the sites is weak password we focused on increasing and improving the level of the security of the site. In this article first we studied the works done in the field of the security of cyberspace of sites to know the level of the users' satisfaction, then by generating a fuzzy inference system improve and increase the security of the password. This system with its the best properties can provide security of site's manager password and can prevent unauthorized access. We have done a comparison by system logs mechanism that the result was the efficiency of it because by increasing the level of security we could decrease system logs mechanism for each site. In future we want to increase the volume of the database and increase the standards of inputs proportionally of course to do so we should define and decide rules more than these.

References

[1] C. Gables, "Cyber Security Metrics, "Enterprise Risk Management Inc, Vol. 2, pp. 1-4, 2012.
[2] Department of Justice, "2012 Internet Crime Report," Internet Crime Complaint Center, PP.13-20, 2013.
[3] D. Spann, M. Craig, and M. Awyong, "Anti-Fraud Resource Guide," ACFE, Vol. 1, pp. 5-9, 2014.
[4] E. Golzardi, M. Meghdadi, and A. Ghaderzade, "Improving Ranking Persian Subjects in Search Engine Using Fuzzy Inference System," IJMEC, ISSN. 2305-0543, Vol. 3(9), PP. 330-344, 2013. J. Farley, "Internet Scam Guide," U.S. Securities and Exchange Commission, pp. 1-8, 2013.
[5] K. Blanton, "The Rise of Financial Fraud: Scams Never Change but Disguises Do," FINANCIAL Security Project, pp. 4-9, 2012.
[6] K. Dadashtabar Ahmadi, A. Rashidi and M. Barari, " The Impact Analysis of Modeling Errors for Projecting Cyber Attacks," IJMEC, Issue. 15, Vol. 5 (15), PP. 2135-2150, 2015.
[7] K. Tripathi, and M. Pavaskar, "Survey on Credit Card Fraud Detection Methods," IJETAE, ISSN. 2250-2459, Vol. 2, pp.1-6, 2012.
[8] M., Awyong, "Merchants Struggle Against an Onslaught of High-Cost Identity Fraud and Online Fraud, "LexisNexis, pp. 4-7, 2013.
[9] Metropolitan police, "The Little Book of Big SCAMS," The Metropolitan Police Service, Vol. 2, pp. 22-35, 2013.
[10] M. Fleming and E. Goldstein," Metrics for Measuring the Efficacy of Infrastructure -Centric Cyber security Information Sharing Effort", HSSAI, 11-01.02.02-01, pp. 8-16, 2012.
[11] N. Modiri and M. Jangjoo, "Engineering of the security of networks of computer, "Mehregane Ghalam, Vol. 4, pp. 227-228, 1392.
[12] R. Akella, H. Tang, and B. Mcmillin, "Analysis of Information Flow Security in Cyber Physical systems," ELSEVIER, 65409-0350, pp. 157-173, 2010.
[13] R. Pooley and B. Palmer, "What Is The Insider Threat, "The Security company International, Vol.1, pp.3-8, 2013.
[14] S. Band, D. Cappelli, L. Fischer, A. Moore, E. Shaw, and R. Trzeciak, "Comparing Insider IT Sabotage and Espionage: A Model-Based Analysis, " Software Engineering Institute, ESC-TR-2006-091, pp. 61-69, 2006**.**
[15] S. Shrum, M.J. Mazzafro, and M. Awyong, "A Preliminary Examination of Insider Threat programs in the U.S," INSA, Vol. 1, pp. 10-15, 2013.
[16] S.Z. Rajabi, S.J. Mirabedini Shirazani and A. Haronabadi, "Detection of Spoofing Attack," IJMEC, ISSN. 2305-0543, Vol. 4 (12), PP. 1366-1377, 2014.
[17] Z. Komorosky, "Dating Sites are Full of Scammers, "Internet Fraud Complaint Center, pp.1-15, 2014.

Authors

Dr. Nasser Modiri (PhD), CEO Ayandegane Computer Co.

Eng. Raheleh Shariatpanahi, M.Sc degree on Computer Engineering-software