# A New Approach to Quantify Network Security by Ranking of Security Metrics and Considering Their Relationships

Mostafa Behi[1], Mohammad GhasemiGol[2], and Hamed Vahdat-Nejad[2]

*(Corresponding author: Mohammad GhasemiGol)*

Department of Computer Engineering, Science and Research branch, Islamic Azad University[1]
Birjand, Iran
Department of Computer Engineering, University of Birjand[2]
South Khorasan Province, Birjand, A78, 97175615, Iran
(Email: ghasemigol@birjand.ac.ir)

*(Received May. 20, 2016; revised and accepted Sept. 3, 2016)*

## Abstract

There are several characteristics in computer networks, which play important roles in determining the level of network security. These characteristics known as security metrics can be applied for security quantification in computer networks. Most of the researches on this area has focused on defining the new security metrics to improve the quantification process. In this paper, we present a new approach to analyze and quantify the network security by ranking of security metrics with considering the relationships between them. Our ranking method reveals the importance of each security metric to quantify security in the network under surveillance. The proposed approach helps the network administrators to have a better insight on the level of network security

*Keywords: Correlation; Regression; Security Quantification; Security Metrics*

## 1 Introduction

In today's digital age, every organization, regardless of its size, must have an information security program to protect its data. This program should be designed in a way to detect, prevent and significantly reduce the risks. Developing a comprehensive information security program that recognizes these risks is one of the major issues that organizations are faced with today. Identification of incidents that has an effect on the organization's assets is one of the important parts of the security program and also a difficult task. The complexity of today's computer networks has made this issue a more complicated process. Since the budgets and resources are often limited in organizations, then a mechanism should be chosen for the right direction of those matters. In [9] Verizon reports that 97% of the attacks could be neutralized by little try because they were done by amateur attackers without so much skills and tools. In spite of the big amount of money spending on security and defense in many organizations, hackers can lower their level of security and confidentiality just by using simple exploit accessible online. Then using right minimums is much better than useless maximums in security. Installing expensive firewalls and UTMs, antiviruses, intrusion detection systems and intrusion prevention systems (IDS/IPS) would be all ineffectual in network security, if one simple task such as users' loss of knowledge about security is misunderstood. In such a case an unaware user can endanger all the organization's network just by using an infected USB memory or connecting an unsecure wireless network to the organization's network or visiting unsecure websites and downloading malicious contents to the network. By network quantification, the current status of the network security would be obtained much more precisely in a way which by it can be compared to different networks' security and the security of the network itself on a timeline base. Prioritization of network attributes based on the numeric effectiveness of each attribute on the network security score causes the efforts to a higher security to be more purposive and less error-prone. Economizing time and other resources on the security is the other important role of security quantification. The quantification of network security in this paper is done by using security metrics.

According to the national institute of standards and technology metrics are tools designed to improve determination, decision and responsibility by gathering, analyzing and reporting the related functions. In other word metrics are standard of measurement which can be used to measure the security level of an organization. Security

metrics are chosen according to the organization needs and security rules. A good security metric [8] should be specific, measurable, attainable, repeatable and time-dependent. There are some different categories of security metrics which can be considered in network security quantification such as:

- Software-based;
- Network-based;
- User-based;
- Policy-based.

One of the most important problems to increase network security is the absence of solutions to measure the relative effectiveness of different security attributes and metrics on the security level of a typical computer network because what is not measured is not controllable [2, 15]. In such a situation, a network security metric is useful because it would provide quantification and measurement supplied by different network attributes. By employing security metrics in a computer network, the administrators can find out which attributes should be more concentrated to increase security while resources consumption is decreasing. A computer network has numerous attributes and metrics which many of them are less important and time consuming to be analyzed.

Then by considering security metrics relationships, the less important ones can be omitted and those which are correlated more to the network security level are kept strongly. Every vendor and company which provides security solutions such as firewall, IDS/IPS, antivirus, UTM for other companies claims that its approach to security is the best, but unfortunately there is no quantitative way to assess their products. The approach presented in this paper tries to show the effect of security metrics individually on the security of the whole computer network by evaluating the relationships between security metrics.

The remainder of this paper is organized as follows. The related works are reviewed in Section 2 and the proposed approach to security quantification is described in Section 3. An experiment of the network security quantification's solution is carried out in Section 4, and finally the paper is concluded in Section 5.

## 2 Related Works

Most of the works in the network security quantification is about identifying an appropriate set of security metric. Ahmed et al. [1] gathered a set of metrics based on vulnerable networks previously found. The authors quantified the present vulnerabilities and their characteristics and estimated the future vulnerabilities in the networks and its services. In another study [18] all misconfigurations and weaknesses which causes the network to be vulnerable to the attacks are studied. By introducing a new metric called VEA-bility security metric, as a comparison tool for different network configurations in order to select the best adjust in the security of the network. A network administrator tries to have the less vulnerable network configuration and of course the more secure one, therefore the writers try to deliver different network configurative comparisons to help the users to choose the best ones. Attack graph-based security metrics are used in [5] to measure the probability of network exploitation according to number of successful attacks done. The network resistance which an attacker is faced with is one of the metrics the authors used. In all the works done in security quantification, the effect of attributes in the network that an administrator is daily faced with are not taken into consideration for determining the level of security.

One important reality should not be forgotten that things which are not measurable are not controllable. In another research [19] researchers by means of attack graph and defining two security metric called probabilistic security metric and attack resistant metric to evaluate the security level of the network. Common vulnerability scoring system has an important role in risk evaluation of the network. This system as described in [13] and [12], is an important step toward network security quantification. The standardized vulnerability scores, open and clear structure for security vulnerability scoring and prioritization of risk identification are the most important features of this system. In [10] the author is describing a way to rank the security metrics based on decision theory and probability distribution. A self-assessment architecture that prepare a solution for the users to determine security metrics that are specially feasible for the user's ISMS is presented in [7]. Then a metric catalogue involving 95 metrics from different sources is provided. In [14] the basic aspects of security metrics are covered. Matters such as definition of security metrics, their value, and difficulties in generating them and a methodology for building a security metric program are expressed briefly. The author in [16] describes some important features and goals of security metrics. Attack graph-based security metrics are used in [6] to measure the probability of network exploitation according to number of successful attacks done. The network resistance which an attacker is faced with is one of the metrics the authors have used in this work.

In [17] taxonomy of Intrusion Response Systems (IRS) and Intrusion Risk Assessment (IRA), two important components of an intrusion detection solution are represented. A self-assessment framework that permits a user to determine the security metrics that are feasible for the user's ISMS is discussed in [7]. In [11] a method to improve the network security, which consists of the network management, the vulnerability scan, the risk assessment, the access control, and the incident notification is introduced. In [3] a risk estimation model based on publicly available data, the Common Vulnerability Scoring Systems (CVSS) is proposed. In [4] a big amount of information is gathered by focusing on three European countries for more than a year and a half through 5 vantage points with different access technologies to make a quantitative

Table 1: The variables that are used in correlation

| r | Correlation |
|---|---|
| $M_1, M_2$ | The value of security metrics |

measurement on the behavior of users with the Internet to gain important metrics.

## 3 The Proposed Approach for Security Quantification

To quantify the network security, a mathematical-based approach using regression and correlation proposed in this paper. Regression and correlation makes possible analyzing the relationships between security metrics in the model of network security quantification. In Figure 1 the structure of this approach is shown.

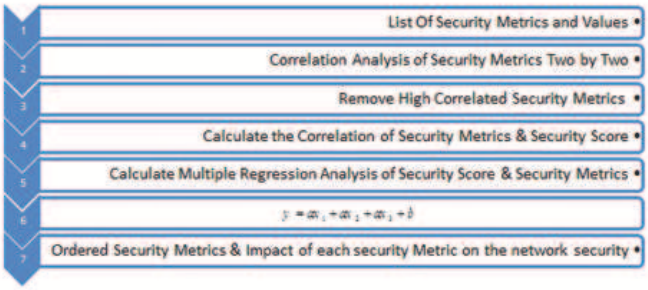



Figure 1: The structure of proposed Network Security Quantification Model

In this structure, the security of the network obtained through three important phases. First, the correlation between security metrics two by two is calculated. In this phase to prevent from multicollinearity[1], one of those metrics which are more correlated to the other one is omitted. By this strategy, just those metrics which are more important and effective to the security remains in the model of quantification. The lesser correlation value between security metrics, the more accurate would be the results of regression model of network security quantification. Figure 2 shows all the correlations between metrics that considered.

Equation (1) calculates the correlations of security metrics two by two.

$$r = \frac{\sum M_1 M_2}{\sqrt{\sum M_1^2 \sum M_2^2}} \tag{1}$$

In this equation the variables are assumed according to Table 1.

At the next phase, the correlations of security score and security metrics two by two are calculated. In this step, the more the value of correlations with the security score the more suitable would be the quantification model of network security. Since correlation is not a cause and effect concept then it just imply the presence of relationship between two security metrics therefore the effect of one specific security metric to the security score of the machine will not be concluded. Then in the next phase by means of regression, the effect of security metrics on the security score is calculated. By implementation of regression, the model of network security would be like Equation (2):

$$SecurityScore = b_0 + b_1 M_1 + b_2 M_2 + ... \tag{2}$$

In which $M_i$ is the value of different security metrics and $b_i$ is the coefficients that expresses the impact of security metrics on the security of the network. In the statistical models, regression evaluation used to study the relationship of variables in a cause and effect method. In the model of network security quantification the security score is the dependent variable and the security metrics are the independent variables. In a regression model, the effect of each independent variable on the dependent variable analyzed. By use of Equations (6) and (7) the coefficients in Equation (4) would be calculated.

$$b_i = \frac{\sum[(M_i - \overline{M})(SS_i - \overline{SS})]}{\sum[(M_i - \overline{M})^2]} \tag{3}$$

$$b_0 = \overline{ss} - b_1 \overline{M}. \tag{4}$$

In these equations the variables are according to Table 2.


Figure 2: The correlation of Metrics

## 4 Experiment

In this study, an organization's network involved about 100 machines, monitored in about two weeks to identify suitable network's security metrics. Fortunately, whole

[1] In statistics, multi-collinearity is a phenomenon in which two or more predictor variables in a multiple regression model are highly correlated.

Table 2: The list of variables used in coefficient of regression

| | |
|---|---|
| $b_i$ | The regression coefficients |
| $M_i$ | The observation $i$ of security metrics |
| $SS_i$ | The observation $i$ of security score |
| $\overline{ss}$ | The average of security scores |
| $\overline{M}$ | The average of security metrics |

the network configurations and also its machines were accessible with appropriate privilege to be investigated in order to extract the security metrics else all the traffic in this period should had been saved to be interpreted later with an offline method. The point of security metrics is not to collect huge amount of data. A small set of data, understood well and usable, would be much more valuable than a pile of data left untouched on shelves or hard drives gathering dust. In this paper, the GQM method employed to develop security metrics. GQM is a simple and three-step process to gain appropriate security metrics for the network. The first step in the process involves defining specific goals that the organization hopes to achieve. These goals are those the organization by quantification is going to reach. Finally, these questions answered by identifying and developing appropriate metrics. This method guarantees that all the metrics identified are according to the goals of the organization. After an act of investigation of the network and by doing some interviews by the network's administrators and users according to the GQM method some more important security metrics chose. In [18], the writer expresses the characteristics of a good security metric such as: consistently measured, cheap to gather, expressed as a cardinal number or percentage and specific.

## 4.1 Web Browser Version (Browser)

Since most of the attacks that a machine is faced with is from the internet and web browsers are the first applications are to the target of attackers, then the web browser version is taken into consideration as a security metric. For each machine on the network the value for this metric is calculated by:

$$WebBrowser = LastVersion - UserVersion. \quad (5)$$

The difference between last version of a specific version and user's browser version is the value allocated to this metric for each machine on the network. In cases more than one browser is used the average of the values is allocated for this metric. Of course in the experimented network the browser which was used according to the security policy of the organization was IE and Firefox. Figure 3 shows the statistics of common browsers used in the organization's network.

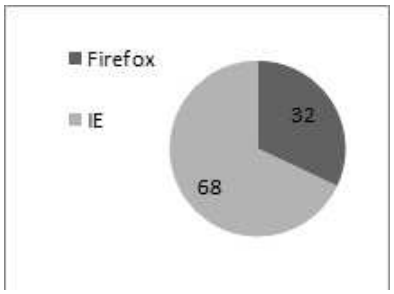



Figure 3: The web browsers statistics

Table 3: The assumed values for various OS

| XP-SP1 | XP-SP2 | XP-SP3 | 7 | 8 | 8.1 |
|---|---|---|---|---|---|
| 5 | 4 | 3 | 2 | 1 | 0 |

## 4.2 Operating System Version (OS)

Since operating system is the infrastructure software for other applications and services to be executed properly, then keeping machine's OS updated is one of critical metrics, which should be considered to have a secure network. The value used for this metric in evaluations presented in Table 3.

All of the operating systems used in the experimented network were different versions of Microsoft windows and they were evaluated according to Table 3. For example, if on a machine win 8.1 is installed the value considered for it is 0 and if win XP-SP1 is installed the value would be 5. It means the higher version of OS the lower numeric specified for that version.

## 4.3 Vulnerabilities (VUL)

By running Nessus vulnerability scanner on the machines, the number of vulnerability on each machine is going to be in consideration as a security metric. Nessus is the world's most popular vulnerability scanner [5] and in 2005 used in 75000 organizations.

## 4.4 Malwares (malware)

By using licensed antivirus's reports, the number of malwares on the machine was obtained. On the experimented network an updated licensed NOD32 antivirus is installed. The server's side of this antivirus has several features, which can report the malwares penetrated into the machine. The value of this metric is the total number of observed malwares on the clients.

## 4.5 Defense Update (Def-Update)

Since the number of new threats continues to grow steadily, then antivirus' being-updated is so important to have a healthy network. The value allocated to this metric is the total number of days past from the last up-

Table 4: The list of variables used in the security score calculation

| | |
|---|---|
| n | The number of machines |
| severity ($v_i$) | The severity for the vulnerability $i$ |
| $Securityscore_i$ | The security score for machine $i$ |

Table 5: The correlation of Security Metrics

| | Browser | OS | Malware | Def-Update | Last-Scan | Update | VUL |
|---|---|---|---|---|---|---|---|
| VUL | 0.09 | -0.09 | 0.08 | 0.03 | 0.21 | -0.35 | - |
| Update | -0.30 | -0.42 | -0.014 | -0.03 | 0.00 | - | -0.35 |
| Last-Scan | 0.05 | -0.13 | -0.03 | 0.24 | - | 0.00 | 0.21 |
| Def-Update | -0.11 | -0.03 | -0.11 | - | 0.24 | 0.03 | 0.03 |
| Malware | 0.11 | 0.19 | - | -0.11 | -0.03 | -0.14 | 0.08 |
| OS | 0.43 | - | 0.19 | -0.03 | -0.13 | -0.42 | -0.09 |
| Browser | - | 0.43 | 0.11 | -0.11 | 0.05 | -0.30 | 0.09 |

date of client's side of antivirus. This value obtained by checking the update part of each antivirus.

### 4.6 Last on-demand scan (Last-scan)

Periodically scanning of the machines in a network is one of the main issues, which can help the network cleanness of malwares and vulnerabilities. Therefore, the total number of days past from the last scan of the network by the antivirus has been taken into account as an important security metric.

### 4.7 Software Updates (Software)

This metric value is the total number of OS and frequently used applications updates according to the security policies in the network. The updates can be managed and obtained by soft wares such as WSUS.

### 4.8 Security Score (security-score)

In order to implement the level of security in the security quantification model, a security score is going to be calculated. The more security score for each machine, the higher the level of security in the network. To calculate security score for each machine, all the vulnerabilities in each machine extracted by using Nessus vulnerability scanner.

Then to obtain the severity of each of the vulnerabilities, they mapped to the NVD[2] one by one. In the NVD, all the vulnerabilities are stored with a CVSS[3]-based severity, which is a number between 0 and 10. According to the Equation (6) the security score for each machine is calculated.

$$Securityscore_i = \sum_{i=1}^{n_k} (10 - severity(v_i)). \quad (6)$$

The variables of Equation (6) is explained in Table 4.

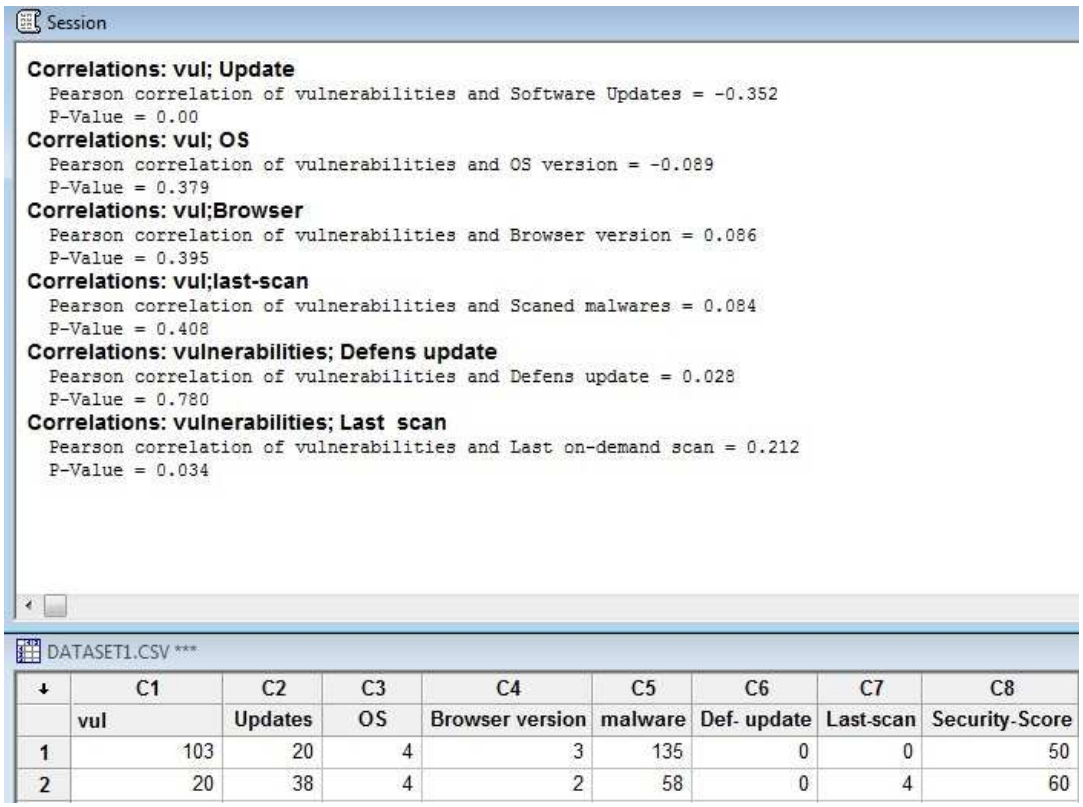
With the help of the theoretical development done in Section 4, now the numeric effect of security metrics on the network security level is going to be calculated.

In this research, the Minitab software version 16 used to interpret the relationship of security metrics. As clarified before the correlation of the security metrics is calculated to avoid multi-collinearity and the results are shown in Figure 4 and Table 5. Correlation of all the security metrics showed in Table 5 to show the non- cause and effect manner of this evaluation. As it is obvious, in Table 5, the correlation of to security metrics Update and VUL is a negative number and it shows that they are correlated in a reversed manner or better to say the more updates taken by the machines, the lesser vulnerabilities found on, or the correlation of two other security metrics VUL and Last-scan is a positive number meaning, the longer time lapsed the last scan, the more vulnerabilities found on the clients. A quick consideration of data in the last table reveals that the results exactly coincides the expectations in the real world.

After evaluating of the correlation between security metrics two by two, the correlation of security score and security metrics should be analyzed. Table 6 contains the result of correlation of security metrics and security score. In this table P-value is also considered by which the results can be better proved. The P-value would reject the null hypothesis[4], if its value was less than the alpha level which is important in the null hypothesis theory. In the other word for the P-Values less than alpha level the null hypothesis is rejected and it shows there is a meaningful relationship between two variables. Figure 5. shows the correlation of security metrics and security scores taken from Minitab. Scatter plots also can be implemented to visualize the correlation of security metrics and security scores. In Figure 6 the correlations of security metrics

[2]National Vulnerability Database:www.NVD.com
[3]Common Vulnerability Scoring System

[4]The term "null hypothesis" usually refers to a general statement or default position that there is no relationship between two measured phenomena, or no difference among groups and variables




| ↓ | C1 | C2 | C3 | C4 | C5 | C6 | C7 | C8 |
|---|---|---|---|---|---|---|---|---|
| | vul | Updates | OS | Browser version | malware | Def- update | Last-scan | Security-Score |
| 1 | 103 | 20 | 4 | 3 | 135 | 0 | 0 | 50 |
| 2 | 20 | 38 | 4 | 2 | 58 | 0 | 4 | 60 |

Figure 4: The correlation of security metrics generated by Minitab

Table 6: The correlation of Security Metrics

| | Browser | OS | Malware | Def-Update | Last-Scan | Update | VUL |
|---|---|---|---|---|---|---|---|
| Security score | -0.26 | -0.21 | -0.37 | 0.1 | -0.26 | 0.38 | -0.23 |
| P-value | 0.01 | 0.03 | 0.00 | 0.3 | 0.3 | 0.00 | 0.02 |

and security scores is illustrated by scatter plot.

As it is evident in the Figure 6 according to the trend line of scatter plot the correlation of security metrics and security score is obvious. For example the positive slope of trend line in scatter plot of Def-update and security scores illustrates as Def-updates increases the security score is also increased and the negative slope of trend line for Malwares and security scores means as number of malwares increases the security score decreases.

## 4.9 Numeric Effect of Security Metrics on the Security Experimented Network

Since correlation is not a cause and effect evaluation, then by means of regression evaluation the exact numeric effect of each security metric on the security score is calculated. In the quantification model of network security Security-Score is dependent variable and the security metrics are the independent variables of the model in which we are going to calculate the effect of them on the security score. Finally, the multiple regression equation expresses the numeric effect of security metrics on the security level of the network. Equation (7) is the regression equation of the quantification model of the network security.

$$\begin{aligned} Security - Score = 56.4872 - (0.211009)Vulnerability \\ +(0.525058)Update + (0.343473)OS \\ -(0.345093)Browser - (0.0300952)Malwares \\ +(0.0511584)Def - update - (0.0575463)Last - scan. \end{aligned} \quad (7)$$

The Equation (5) is the quantification equation of the network security in which the coefficients are the numeric effect of each security metric on the security when the other metrics are assumed as 1. The Figure 7 illustrates this model calculated in Minitab software.

According to Equation (5) the order of security metrics according to their effect on network security is gathered in Table 7. The security metric Updates has the most effect on the security score with coefficient 0.52 and the Web browser, OS and Vulnerabilities are the next more important security metrics orderly.

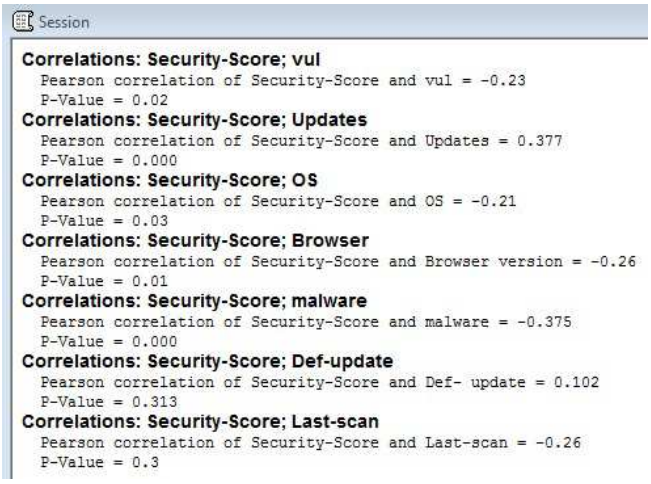



Figure 5: Correlation Of security metrics and security score

Table 7: The correlation of Security Metrics

| Rank | Security Metrics | The Importance Value |
|---|---|---|
| 1 | Updates | 0.52 |
| 2 | Browser | 0.3451 |
| 3 | OS | 0.3435 |
| 4 | Vulnerabilities | 0.21 |

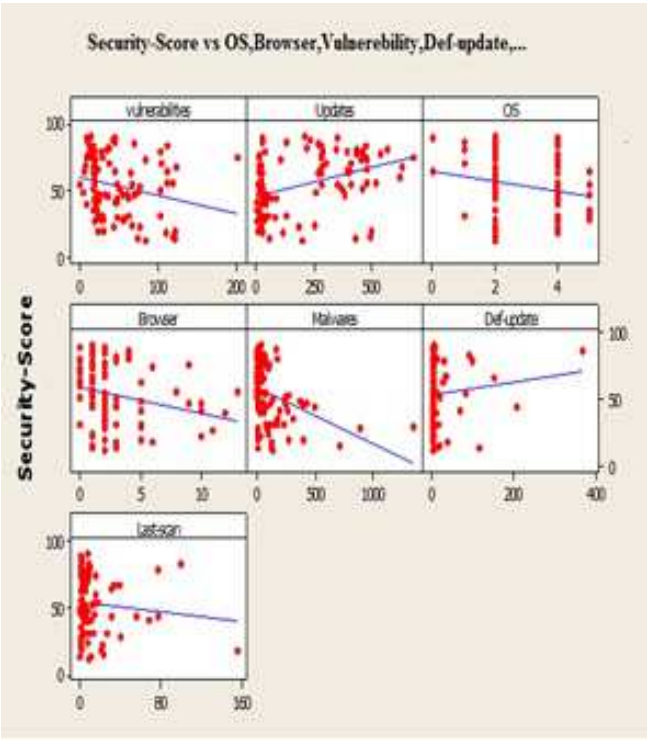



Figure 6: The scatter-plot of security score and security metrics

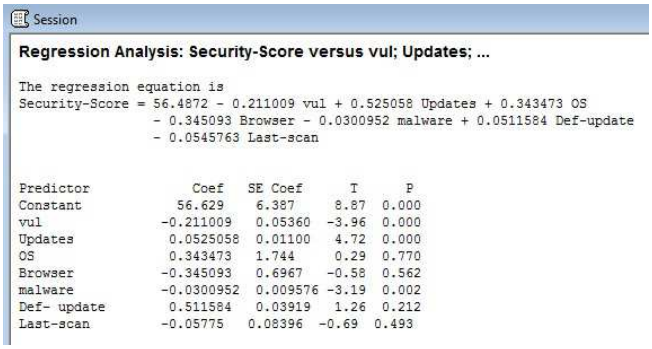



Figure 7: The regression model of network quantification

## 5 Conclusion

This paper is going to provide a structure for quantification of network security and prioritization of significant security metrics. A mathematical approach is developed that can help to quantify the network security and order the security metrics. By implementing regression and correlation to the network security era and security metrics the quantification of network security will be possible as shown in this paper. Once the security quantification is done, administrative efforts can be concentrated to increase security more precisely and efficiently. As it is shown in this paper there are some relationships between network attributes or security metrics which by evaluation of them the network administrators can manage the network more efficiently.

## References

[1] M. S. Ahmed, E. Al-Shaer, and L. Khan, "A novel quantitative approach for measuring network security," in *The 27th IEEE Conference on Computer Communications (INFOCOM'08)*, pp. 1957–1965, 2008.

[2] A. Anurag, "Network neutrality: Developing business model and evidence based net neutrality regulation," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 1–9, 2015.

[3] G. A. Franca III, "Baseline operational security matrics for industrial control system," in *Proceedings of the International Conference on Security and Management (SAM'16)*, p. 8, The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing, 2016.

[4] J. L. García-Dorado, A. Finamore, M. Mellia, M. Meo, and M. Munafo, "Characterization of ISP traffic: Trends, user habits, and access technology impact," *IEEE Transactions on Network and Service Management*, vol. 9, no. 2, pp. 142–155, 2012.

[5] H. Ge, L. Gu, Y. Yang, and K. Liu, "An attack graph based network security evaluation model for hierarchical network," in *IEEE International Conference on Information Theory and Information Security (ICITIS'10)*, pp. 208–211, 2010.

[6] N. Ghosh and S. K. Ghosh, "An approach for security assessment of network configurations using at-

tack graph," in *IEEE First International Conference on Networks and Communications (NETCOM'09)*, pp. 283–288, 2009.

[7] B. Heinzle and S. Furnell, "Assessing the feasibility of security metrics," in *International Conference on Trust, Privacy and Security in Digital Business*, pp. 149–160, Springer, 2013.

[8] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*, Addison Wesley, 2007.

[9] H. Kahtan, N. A. Bakar, and R. Nordin, "Dependability attributes for increased security in component-based software development," *Journal of Computer Science*, vol. 10, no. 8, pp. 1298–1306, 2014.

[10] M. Khan, M. Omer, and J. Copeland, "Decision centric identification and rank ordering of security metrics," in *IEEE 37th Conference on Local Computer Networks (LCN'12)*, pp. 208–211, 2012.

[11] Y. P. Lai and P. L. Hsia, "Using the vulnerability information of computer systems to improve the network security," *Computer Communications*, vol. 30, no. 9, pp. 2032–2047, 2007.

[12] P. Mell and K. Scarfone, "Improving the common vulnerability scoring system," *IET Information Security*, vol. 1, no. 3, p. 119, 2007.

[13] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security & Privacy*, vol. 4, no. 6, pp. 85–89, 2006.

[14] F. Nielsen, "Approaches to security metrics," in *CSSPAB Workshop on" Approaches to Measuring Security*, 2000.

[15] E. U. Opara, O. A. Soluade, "Straddling the next cyber frontier: The empirical analysis on network security, exploits, and vulnerabilities," *International Journal of Electronics and Information Engineering*, vol. 3, no. 1, pp. 10–18, 2015.

[16] S. C. Payne, "A guide to security metrics," *SANS Institute Information Security Reading Room*, 2006.

[17] A. Shameli-Sendi, M. Cheriet, and A. Hamou-Lhadj, "Taxonomy of intrusion risk assessment and response system," *Computers & Security*, vol. 45, pp. 1–16, 2014.

[18] M. Tupper and A. N. Zincir-Heywood, "Vea-bility security metric: A network security analysis tool," in *Third International Conference on Availability, Reliability and Security (ARES'08)*, pp. 950–957, IEEE, 2008.

[19] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An attack graph-based probabilistic security metric," in *IFIP Annual Conference on Data and Applications Security and Privacy*, pp. 283–296, Springer, 2008.

# Biography

**Mostafa Behi** joined central office of Communication and Information Technology (ICT) of South Khorasan province as an IT Expert on summer 2014. He received his MS degree in computer's software engineering from Azad university of Birjand and his B.S degree from university of Birjand. He mostly researches on network security, cloud computing and data mining.

**Mohammad GhasemiGol** will join the Department of Computer Engineering at the University of Birjand on fall 2016. He received the B.S. degree in Computer Engineering from Payame Noor University (PNU), Birjand, Iran, in 2006. He also received the MS and PhD degree in Computer Engineering at FUM, Iran, in 2009 and 2016 respectively. November 2014 to July 2015, he was with the Department of Computer Science and Engineering, University of North Texas, Denton, TX, USA as a visiting research scholar. His research interests include network security, intrusion detection and response systems, alert management, data mining, and optimization problems.

**Hamed Vahdat-Nejad** is currently an assistant professor at the computer engineering department of the University of Birjand. He received his PhD from computer engineering department of University of Isfahan in 2012, his master degree from Ferdowsi University of Mashhad in 2007, and his bachelor's degree from Sharif University of Technology in 2004. He was a research scholar at the Middleware laboratory of Sapienza University of Rome in 2011. Currently, his research is focused on cloud computing, pervasive computing and security. He has (co)published about 30 papers in conferences and journals, and leads the Pervasive and Cloud computing Lab at the University of Birjand. He has served as the chairman of the 1st and 2nd International Workshop on Context-aware Middleware for Ubiquitous Computing Environments, as well as the 3rd and 4th International workshop on Pervasive and Context-aware middleware. He has served as TPC member for ICCKE, IWCMC, ISIEA, ICCIT-WCS, PerCAM, ChinaCOM, MELECON2014, COGNITIVE-2014, IBMSGS2015, EMERGING 2015, ICACCI, ADMMET'2015 ICCME-2015, CoCoNet'15, AR4MET'2016, REEGETECH'2016, ISTA16, etc. Currently, he serves as associate editor for Elsevier Computers and electrical engineering journal.