Development of Secure Network System for Complex Network

Johnson Uche Olu-Egbuniwe
PhD Candidate
Girne American University
Turkey

Samson OluwaseunFadiya
PhD Candidate
Girne American University
Turkey

Abstract

This paper looks at the significance of the implementation of visualization technique in the development of a secure network on complex networks; also the effects of certain factors like the level of trained staff and IT budget allocation upon implementation of this technique, as well as their effects on complex networks. Descriptions of the techniques used to protect and keep PC's up and undisturbed. Protecting the clients' security and privacy is of high priority. This paper sets to look at the internal and external security challenges in businesses and corporations that implement both wireless networks wired networks. With the introduction of cloud computing, the risks of viruses, worms and hackers has increased. The use of distributed security is designated to fully cover and provide more security over data that is shared among faculty members, colleagues, clients and any other user within the cloud. The problems and issues enlisted by Cisco and Microsoft are reviewed and help in aiding the proposed project route. The research showed that that the funds allocated to security in the IT budget is important. The level of trained IT staff showed greater importance for the implementation of visualization in a complex network.

Keywords: Network Security, Complex Networks, Visualization, IT budgets, trained staff level

1.0 Introduction

The advancement in technology and the quest to effectively and efficiently serve clients has enabled organizations to implement information technology. Information technology coupled with networking enables organizations to communicate easily and share resources. Networking allows users to access servers which are protected by their operating system gatekeepers. With the many hackers and malicious software trying the much they can to compromise security of network systems, network security is a major concern (McClure et al. 2003).

Network security involves applying various security measures to protect network devices such as routers, firewalls, and switches in order to secure data. Unsecured network may allow hackers and competitors to access organizations' critical information or destroy data. Just like organizations' assets such like employees data is very important and their loss can greatly affect organizational performance. Various security measures such as passwords, Mandatory Access Control (MAC), Discretionary Access Control (DAC), and firewalls have been put in place to secure networks (Frouzan, 2001).

Networks that aim at maintaining confidentiality of their data is usually affected by usability. But for networks whose aim is privacy, usability becomes very important as it aims at hiding both the data being communicated and the system communicating. This is normally the case for networks with many users and requires high levels of security such as those for law enforcement and government intelligence agencies.

Though there are many network security measures such as encryption, password protection, and firewalls in place, they are difficult to implement in complex networks, which can be solved by visualization.

1.1 Background of the Study

Network security has been a major concern since the development of computer networks. Information transferred over a network can be intercepted, eavesdropped, or changed before reaching destination. Since there were no ways of detecting what was going on in the networks, organizations experienced many damages including loss of data, duplication of data, password changes, server blocks, etc.

On realizing this, many researchers developed various means of securing networks which include firewall installation, password use, encryption algorithm use, physical protection, antispyware installation, and MAC address filtering (Pratt, 2003). Since the measures were specifically meant for small networks, they become difficult to secure complex networks. Moreover, hackers work around the clock to compromise them, which raise concerns on their level of security. Researchers, on the other hand, work hard to ensure the measures are reinforced to prevent networks from being compromised.

1.2 Problem Statement

While the importance of securing networks such as installation of firewalls, encryption, use of antispyware, and use of passwords (Meire, 2003) cannot be overruled, implementing them in complex networks becomes a problem. They require a lot of time and resources to implement and can be vulnerable to attacks.

To solve this, data gotten from questionnaire would be analyzed using the SPSS statistics

1.3 Research Questions

Organizations with complex networks are normally affected when the current security measures are compromised. To show how analysis of visual data can help secure complex networks, the following questions need to be answered:

i. How important do network administrators consider all aspects of network security?
ii. What are the various security measures in place and how effective are they when implemented in complex networks?
iii. How can visualization data help secure complex networks?

1.4 Relevance of Study

Many organizations are greatly affected when their complex networks are compromised. Though various network security measures such as use of passwords, encryption, and firewalls are implemented, they are normally vulnerable to security breaches. This study comes at the right time as it will develop ways by which visual data analysis would help secure complex networks.

A part from being a partial fulfillment of a degree program, the research will help organizations, network administrators, network designers, and network analysts solve security problems experienced in complex networks.

1.5 Hypothesis Testing

- First hypothesis: Visualization application will have significant influence on complex network.
- Second hypothesis: IT budget will have significant influence on complex network.
- Third hypothesis: Level of trained staff will have significant influence on complex network.

1.6Research Barriers

The study intends to employ both primary and secondary research methods. Primary research will entail preparation and presentation of anonymous questionnaires to chosen target population which will aid in collecting quantitative data. Secondary data will be obtained from different scholarly articles available in the University's library. The collected data will then be analyzed using various data analysis techniques. Getting a favorable and quick response will be needed from the target in order to complete and satisfy all conditions of this research.

2.0 Literature Review

This section reviews various literature related to the research topic to form a foundation of what is to be analyzed and discussed in the research. It discusses basic issues for a secure network and the difficulties that have been faced in design measures of overcoming treats.

2.1 Basic Issues for a Secure Network

Computer networks enable effective communication and sharing of computer resources. As organizations continue to depend on networks for communication, network security threats continue to be a major problem. This has made organizations including governments to respond to such issues by developing test beds, guidelines, security tools, and practicing of best network security practicing to secure their critical information from attacks.

In the past years, networks have experienced increased security breaches including hacking, and malicious threats which either affect their performance or terminate their operations. Network systems are subjected to various threats and vulnerabilities including viruses, worms, Trojan horses, spam, password attacks, sniffing, and hardware attacks (Rigney, et al. 2000). According to Zhou and Haas (1999), all the security threats to a network must be considered, before designing or deciding on the best control measures to implement.

Various security measures have been put in place to ensure networks are secure from attacks. Authentication protocol helps authenticate identity of users (Smailagic et al., 2002) to avoid impersonation. Three common authentication protocols are Kerberos, RADIUS, and EAP. Kerberos protocols targets distributed networks because access to such networks needs a lot of control. In this protocol, authentication is done in a centralized place such as a server to prevent threats which would have been experienced when authentication was done at workstations such as modification of workstation address to identify another user, reply attacks, and identity spoofing (Stallings, 1998).

RADIUS authentication scheme authenticate users to access network devices. It has been successfully implemented in embedded systems especially in cases where access by many users may interfere with normal operations due to low memory capacities (Rigney et al. 2000). RADIUS design, however, degrades performance and leads to loss of data on large systems (Rigney et al. 2000). Extendible authentication protocol supports both point-to-point and multipoint connections. It utilizes IEEE 802 architecture to authenticate switches and access-points (Neskovic, A., Neskovic, N., &Paunovic, 2000).

Traditional measures of securing network such as the use of firewall and encryption algorithm are not sufficient to protect even the smallest networks (Yongguang et al. 2003). Kaderali (2002) adds that the complex nature of computer networks warrants more sophisticated measures to ensure complete network protection. According to Farshchi (2003), threats to networks are numerous and devastating and there is need to design security measures that are upgradable and effective.

Security of complex networks is of concern since it contains many nodes. Nodes present major security vulnerabilities in the way they route packets (Zhou & Haas, 1999). There are threats that include selfish nodes that do not want to do what the protocol wants them to do, and malicious nodes that may disrupt the operations of a network by introducing many attacks.

2.2 Difficulties Faced in Network Design Measures

The various measures which are in place to counter network attacks have experienced various difficulties in their design and implementation. Technology changes rapidly and a delay in design and implementation of such measures finds when new threats have emerged. In addition, hackers work around the clock and come up with ways of compromising systems. According to National Institute of Standards and Technology (2001), unless long lasting solutions that are updatable are found, network security becomes and will remain a major concern.

3.0 Research Methodology

3.1 Data Collection

This research involved questionnaire, observation, and secondary sources to collect data that would help answer the research questions. Questionnaires were sent to 15 reputable companies in Nigeria to attain the results. The 8 questions were directed to the network Administrator in charge of all IT department.

Questionnaire method will be used because it provides the following advantages: Has a standard way of collecting information therefore more objective compared to other methods such as interviews, provides a quick way of collecting data as respondents do not need to engage directly with those collecting data, enables collection of required data or information from a large group, are cost effective when collecting data from a large sample sizes, produces data in a form that is easy to analyze, and provides respondents with enough time to fill them as they can fill them at their own free time.

Secondary sources such as text books and journals were used after thorough consideration of credibility of their authors and publishers. The secondary sources which was used from evaluated scholarly articles to ensure quality of the research. This is because scholarly articles usually pass through expert evaluation before publishing to ensure they meet desired academic standards, contain references, footnotes, and endnotes that support them, and contain descriptions of methodologies used to gather the data used to write them.

Analysis of data is chosen because of the following reasons: Will provide insights concerning operations of current security measures, and highlight what need to be done in the visualization analysis approach to provide secure networks (Sekaran, 2003). In addition, the observation method is flexible and can be formal or informal. This means that the questions can be structured to get specific information from participants or unstructured.

3.2 Data Analysis and Presentation

Table 1:Cronbach Alpha results

Cronbach's Alpha Based on Standardized Items	*N* of Items
.815	8

Cronbach Alpha (α) test was used to find out instrument reliability. The value was = 81.5% for the questionnaire. All values are accepted since they are more than 60% (Malhotra, 2004).

Hypothesis Testing

The hypotheses are tested by the Statistical Package for Social Sciences (SPSS) software.

First hypothesis: Visualization factors will have significant influence on complex network.

Table 2:ANOVA Test for the Effect of Visualization on Complex Networks

Sum of Squares	*df*	Mean Square	*F*	Sig.	*R*	*R* Square
1.028	1	1.028	2.554	.136**	.419	.175

** Significant (*p*) at (0.05) level

Table (2) indicates that *p* calculated value is not significant at (0.05) level. Therefore, Visualization factors will have no significant influence on complex networks with *r* 0.419; also 17.5% of the variance r^2in the complex networks has been not significantly explained by the visualization factors.

Second hypothesis: IT budget will have significant influence on complex network.

Table 3:ANOVA Test for the Effect of ITBudget on Complex Networks

Sum of Squares	*df*	Mean Square	*F*	Sig.	*R*	*R* Square
1.611	1	1.611	4.554	.050**	.525	.275

** Significant (*p*) at (0.05) level

Table (3) indicates that *p* calculated value is significant at (0.05) level. Therefore, IT budget will have significant influence on complex networks with *r* 0.525; also 27.5% of the variance r^2in the complex networks has been significantly explained by the IT budget.

Third hypothesis: level of trained staff will have significant influence on complex network.

Table 4:ANOVA Test for the Effect of Level of Trained Staff on Complex Networks

Sum of Squares	*df*	Mean Square	*F*	Sig.	*R*	*R* Square
2.554	1	2.554	9.276	.010**	.436	.660

** Significant (*p*) at (0.05) level

Table (4) indicates that *p* calculated value is significant at (0.05) level. Therefore, level of trained staff will have significant influence on complex networks with *r* 0.436; also 66% of the variance r^2in the complex networks has been significantly explained by the level of trained staff.

4.0 Discussion of Results and Conclusion

The analyzed data showed that there was significance when there are adequate allocated funds for security in the IT budget on complex networks. Another analysis showed there was significance of much greater value if IT staff are well trained in the complex network.

However, the analysis result on importance of visualization on the complex networks showed that there was no significance. IT administrators have been able to match the day to day challenges with good IT budgets and good level of trained staff. Small companies however do not need to too much budget but will require a good level of IT trained staff to be able to secure the day to day network threats.

Organizations utilize networks to perform their daily functions. Though there are network security measures to counter attacks, network security is a major concern. Researchers should work hard to develop security measures that can identify threats and protect networks in time. This proves that irrespective of the application of visualization, if there is adequate funds and or well trained staff in a complex network, then there is a good security measure in place.

References

Farshchi, J. (2003). *Wireless intrusion detection systems*.

Frouzan, B. A. (2001). *Data communication and networking*, 3rded. New York, NY: McGraw Hill.

Kaderali, F. (2002). Security issues in mobile Applications. *HUT T-110.55 Seminaron Internetworking*, 26/27-04.

Malhotra, N. K. (2004), Marketing research, New Jersey: Prentice Hall.

Marane, A. (2008). *Using Visual Analysis for Network Threat Detection*. Retrieved from http://linkanalysisnow.com/2011/07/using-visual-analysis-for-network.html.

McClure, S. et al. (2003). *Hacking exposed: Network security secretes and solutions*, 4thed. New York, NY: McGraw Hill.

Meier, J. D. (2003). Improving web application security: Threats and counter measures. *Securing Your Network*, 1 (1), 3.

National Institute of Standards and Technology. (2001). *Security self-assessment guide for information technology systems*.

Neskovic, A., Neskovic, N., &Paunovic, G. (2000). Modern approaches in modeling of mobileradio systems propagation environment. *IEEE Communications Surveys and Tutorials*, 2-12.

Pete, H. (2002). *Open-Source Security Testing Methodology Manual*. Sage Publications.

Pratt, J. (2003). A practical guide to the smartphone application security and code signing model for developers. *Windows Mobile software for Smartphones*. 1 (2), 2.

Rigney, C., Livingston, S. W., Merit, A. R., & Daydreamer, W. S. (2000). *RFC265: Remote Authentication Dial IN User Service (RADIUS)*. IETF – Net – work Working Group.

Sekaran, U. (2003). *Research methods for Business: A skill building approach*. NewYork, NY: John Wiley & Sons.

Smailagic, A., Siewiorek, D., Anhalt, J., Kogan, D., & Wang, Y. (2002). Location sensing andprivacy in a context aware computing environment. *IEEE Personal Communications*, 9, 10-17.

Stallings, W. (1998). *Cryptography and network security: Principles and practice*, 2nded. NewYork, NY: Prentice Hall

Yongguang, Z., Lee, W., & Huang, Y.(2003). Intrusion detection techniques for mobile wireless Networks. *Malibu, California*, 1, 16-30.

Zhou, L. & Haas, J. Z. (1999).Securing ad hoc networks. *IEEE Networks*, 12 (6), 22-28.