Volume 2, No. 4, July-August 2011

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Security Measurement Framework: A Network Perspective

Mukta Narang*
Department of Computer Science
Jamia Milia Islamia
New Delhi, India.
mukta.narang@gmail.com

Monica Mehrotra
Department of Computer Science
Jamia Milia Islamia
New Delhi, India.
drmehrotra2000@gmail.com

Abstract- With technology advancements everyday, it is necessary to stay connected and updated. With almost all our confidential data and information on the network, it is important to secure it. Furthermore, it is more important to carefully design a security metric that can give us the confidence to use any network for the same. This study proposes a Security Measurement Framework to find the Security Factor for a network. The Security Factor can give that confidence level to the users/security analyst of a network. The framework involves an in-depth analysis approach to decompose the security of the network into the minutest measurable components. Then security metrics is applied on these components to calculate the final Security factor for the network.

Keywords: Security measurement framework, Security metrics, Network security

I. INTRODUCTION

Websense Security Labs reported that in latter half of 2009, there was a 225percent increase in malicious websites. Worse, 71 percent of these websites were found to be legitimate websites compromised in some way [2]. With Internet becoming a part and parcel of our daily life, do you think that your network could remain unaffected by this huge army of malware, worms, hackers, spyware, viruses, spam, Trojans, rootkits and many more, which are always on the network in search of vulnerable spots? With the growing vulnerabilities each day, one can never be sure of the security of its network. Does this ever stop anybody from accessing Internet or any other network? Then how do we decide which network is safe to visit? Probably gut feeling, word of mouth, reputation in the cyber word, some surveys and news about a network decides how secure it is. Think of it, if we could talk of this in numbers or some figures which state the security factor of a network. That is, if one could quantify security for a network. As Lord Kelvin very rightly said "When you can measure what you are speaking about and express it in numbers you know something about it". [4] Thus the prime focus of this paper is to give a security measurement framework for measuring security factor of a network. To make this paper more focused we have not considered wireless networks here.

II. RELATED WORK

Our earlier work includes the identification of a generic security metrics for all software systems [7]. The work presented in this study is an application of this metrics to networks, emphasizing on the methodology of measuring security.

The U.S. National Institute of Information Standards and Technology (NIST) has recommended Security Controls for Federal Information Systems and organizations in NIST Special Publication 800-53 [6]. ISO Code of Practice for information Security Management (ISO 17799, 27002) [9] recommends some best practices for information security.

The co-author of this study Mehrotra et al. [1] in her earlier work has presented a technical report to DIT, ministry of communication & IT, where they have laid down various security policies. In our framework we are decomposing security to its minutest measurable components. The framework has taken care that these components can be mapped to the most important standards and policies which are followed by various organizations.

III. SECURITY MEASUREMENT APPROACH

Security as stated in wikipedia is the degree of protection against danger, damage, loss, and criminal activity. This definition holds for all network security, computer security, information security, physical security or any other form of security. To secure any location, network, software or information there has to be two basic components. The first one is to identify the weak points/spots which could lead to security breach. Secondly the weight value attached to this vulnerable spot. Take an example of the physical security of an office. If one has to secure an office physically, the first thing is that you analyze the infrastructure of the office building. The next step would be to identify those spots which could allow an intruder inside your building. Once the potential weak spots are identified, we find different ways to secure them. Would you think of the same security measures at all these weak spots? The answer has to be NO. Depending on the security contribution it is decided where could the cameras go and where would there be a security guard and so on. Thus every vulnerable spot cannot be given the same weightage; it varies and also depends upon many parameters.

Applying the above analogy to the security of a network, we propose the following process for measuring security of a network:

A. Identify different dimension of security that can be applied to the network.
B. Identify the major parameters that can be considered under each dimension of security

© 2010, IJARCS All Rights Reserved

C. Using a decomposition approach, identify the basic measurable components for each category of parameters identified.
D. Based on the intensity of importance of different parameters assign weights to each of them.
E. Based on the above gathered data, calculate the security parameter for the network.

IV. SECURITY MEASUREMENT FRAMEWORK

Traditionally, the function of a network has been to deliver packets from one endpoint to another. Processing within the network was limited to routing, congestion control and quality of service. With the advancements coming in, these networks have improved in all respects. The networks now are much more complex with firewalls, web proxies, and multicast routers becoming an integral part of any network. With the growing complexities, the need of security in these networks was established. Network architecture is laid down with Security as its integral part. This is the reason why all our transactions, data, services are shifting to networks. What is still keeping people away from trusting all these networks is the ever increasing security threats. The security measurement framework (fig. 1) is a step towards giving the users of these networks a confidence level in terms of the security factor.

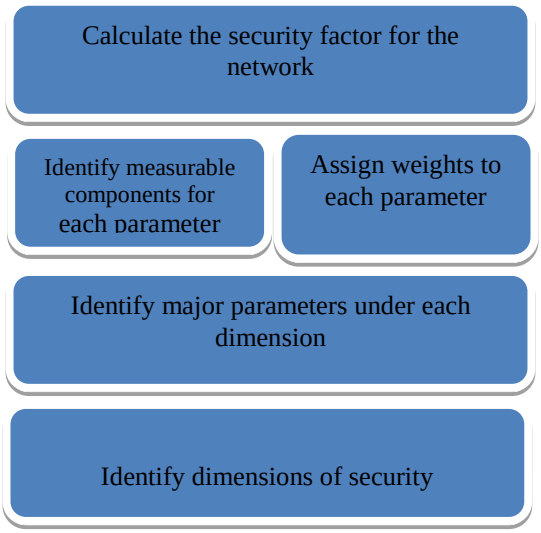

Figure. 1: Security framework for measuring security of network (The approach here is bottom up)

A. *Identify Dimensions of Security*

Before measuring the security of any network, it is very important to understand the architecture of that network from all the aspects of security. Security is a wide concept and has different dimensions. Instead of taking a holistic view of security, it is better to decompose it till we get some measurable components to it. The first level of decomposition could be different dimensions of security. There are basically three dimensions of security (fig. 2) for a network [8]:

a. Physical Security

This includes all the physical access points of the network. A network has to be secured physically at all entry points like main gates, server rooms, workstations.

b. Policy Level Security

Every organization these days is applying some security policy at corporate governance level. The overall objective is to control or guide the human behavior in an attempt to reduce the risk to assets by accidental or deliberate actions [5]. A well implemented security policy at all levels of a network can make your network fully secure. The problem is not abiding by these policies fully which leads to those loopholes for the hackers to enter the network.

c. System Security

This dimension unlike the other two focuses on the system components in a network. This includes security at server, workstation, operating system, firewall and any other component of the network.

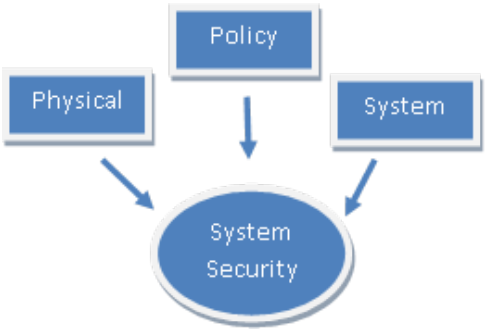

Figure 2: Three dimensions of network security

B. *Identify the Major Parameters Under Each Dimension*

Moving ahead with the decomposition approach, this takes us another step deeper into security of the network. At this level we identify the major parameters which contribute to the above identified dimensions of security. There could be various parameters listed under different dimensions. An attempt has been made to list some major contributors here (fig. 3) [5][6] .

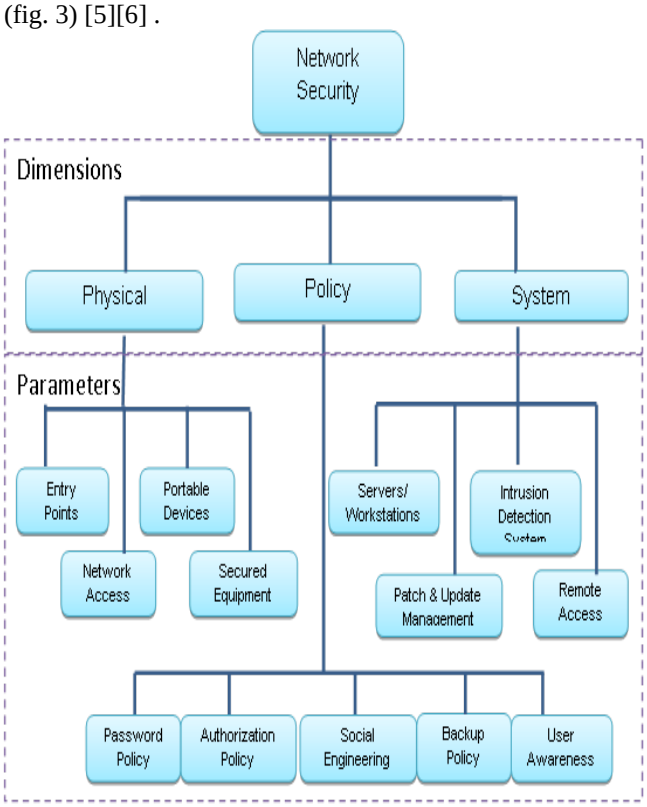

Figure. 3: Hierarchy of network security, showing the different dimensions at level 1 and further the parameters under each dimension at level 2

© 2010, IJARCS All Rights Reserved

C. Identify the basic Measurable Components for Each Parameter

This is the place where we start thinking in terms of numbers, which is quantification of security. By now we have all major contributors of security of a network with us. For each parameter identify a way to quantify it. There could be various approaches to do this. One such approach is to have a series of questions in form of a checklist for each parameter [3]. Each question in the checklist is representing a security action contributing towards that specific parameter. The answers to these questions have to be Boolean, because either the network has taken care of that action or has ignored it due to various reasons like cost, negligence or lack of awareness. Taking the same hierarchy specified in Fig. 3 we will have an exhaustive checklist for each parameter. Each checklist will have some action items. For example the parameter, password policy can have some action items like:

a. Are there some enforced password strength parameters(like atleast 8 characters, some combination of alphanumeric values)[10]
b. Is there any procedure for expiry of passwords after fixed days[10]
c. Is there any procedure to reset password by security administrator on request of user, only after verifying their id[9]
d. Is there enforced changing of default passwords[9]
e. Does the network prohibit the use of default passwords, where applicable[9]
f. Is there proper encrypted backup of all passwords[1]
g. No paper or electronic record of passwords, unless this can be done securely[9]
h. Do passwords remain confidential and not shared ,posted or otherwise divulged in any way[1]

Based on the number of actions items that have been taken care of in this checklist, we can get a value representing the strength factor of the parameter. The strength factor can be calculated using the metric (1):

$$X = C / (T-NA) \qquad (1)$$

Where
X = Strength factor associated with a parameter
C = checked points in the checklist
T = Total checkpoints in the checklist
NA = Not applicable points for the network in the checklist (since the checklist is for any generalized network there could be some action items which are not applicable for any specific network)

D. Assign Weights to Each Parameter

We have different security measures at various vulnerable points. This in itself proves that all potential weak spots do not have the same importance. A security analyst can suggest various security measures at various vulnerable points but there could be various constraints because of which they all are not implemented. These constraints can include cost, technical infeasibility, management is not convinced and many more. The management has to take a wise decision such that the optimal security is implemented at the most nominal cost. Taking all these things into consideration we would ask the people directly involved in the network to assign weights to all the parameter identified. There could be various ways of doing this. We can have two types of weights assigned. The first type is static weights, which could be assigned based on some survey conducted. This would be a tedious task; because it would involve some good number of similar types of networks being analyzed in a tedious manner till some generalized value of weights is achieved. The second type could be dynamic weights which could be assigned using a semantic scale each time an analyst wants to know the security factor associated with a network. This method would involve a one time effort in designing a semantic scale which could be then used for any kind of network. This method would be more feasible because with the ever increasing vulnerabilities, there are fair enough chances that there would be changes in the hierarchy. For a dynamically changing hierarchy, dynamic weights seem to be a better option.

E. Calculate the Security Factor for the Network

For all the parameters, once we have their strength factor and the associated weightage for them, we can calculate the security factor associated with all the dimensions at level 1. The security factor for the dimensions would be calculated using the metric (2) :

$$S_d = \sum_{i=1}^{n} W_i X_i \qquad (2)$$

Where
S_d = Dimensional Security Factor
n = Number of parameters
W = Normalized weights for a parameter
X = strength factor for a parameter

A weighted sum of all the dimensional security factors will give the overall security factor for the network. Thus the overall security factor can be calculated using the metrics (3):

$$S_n = \sum_{i=1}^{N} (S_d)_i \qquad (3)$$

Where
S_n = Security factor of a network
S_d = Dimensional Security Factor
N = Number of dimensions along which security is calculated

S_n would be security factor for the network, which finally explains HOW SECURE IS THE NETWORK. The value of S_n will always lie between 0 and 1. This factor does take care of the security actions actually implemented in the network in terms of 'X' and how important that security parameter is from the analyst point of view in terms of 'W'.

V. CONCLUSION AND FUTURE WORK

Security metrics is an emerging research area rapidly gaining momentum. Security is now in the blood of all software intensive systems and networks. In the future security will be the biggest parameter to judge any system. In this study a novel attempt has been made to achieve the same goal. The security measurement framework proposed in this study is a step by step process to analyze the network from the security perspective and then apply various metrics to get the security factor for any network. Security factor, the end product of this framework should be able to give the confidence to all the users of the network or vice versa.

© 2010, IJARCS All Rights Reserved

Our future work includes further evolution and formalization of the proposed framework. This includes more thorough investigation of suitable generic decomposition model and generic checklists. Furthermore, standardized method to measure security of a network should be developed and validated in actual systems.

VI. REFERENCES

[1] S.I.Ahson, M.Mehrotra, S.K.Panday, S.Rehman, "Technical Report – 2 on Software Security Defects – A Classification Approach", Submitted to DIT, Ministry of Communications & IT, Govt. of India, May 2007

[2] C.Foresman, "All that user generated content? 95% is malware", Ars Technica,February 2010

[3] A.Jaquith, "Sample questions for finding Information Security Weaknesses", CSO Online, May 2007

[4] A.Jaquith, "Security Metrics: Replacing Fear, Uncertainty, and Doubt", Addison Wesley, April 2007

[5] P.Kumar, S.Maheshwari, A.Jain, R.Singh, A.Pruthi, A.Goyal, R.Goyal, "IT security and audit policy", Department of IT Govt. of NCT of Delhi

[6] G.Locke, P.D.Gallagher, "Recommended security controls for federal information systems and organization", NIST Special Publication 800-53,August 2009

[7] M.Narang, M.Mehrotra, "Security Issue – A Metric Perspective", International Journal of Information Technology and Knowledge Management (IJITKM),Volume 3, No. 2,pp.567-571,July-December 2010

[8] L.Parker.L," Fundamentals of network security", Pacific coast information system, 2010

[9] Access Control (ISO 17799-27002) Privacy / Data Protection Project, University of Miami, July 2006

[10] M.Souppaya, J. P. Wack, K.Kent, "Security Configuration Checklists Program for IT Products – Guidance for Checklists Users and Developers", NIST Special Publication 800-70, May 2005.

© 2010, IJARCS All Rights Reserved