Volume 3, No. 3, March 2012

Journal of Global Research in Computer Science

RESEARCH PAPER

Available Online at www.jgrcs.info

ISSN-2229-371X

A NEW METRICS FOR PREDICTING NETWORK SECURITY LEVEL

Tito Waluyo Purboyo*[1], Budi Rahardjo[2], Kuspriyanto[3], and Intan Muchtadi-Alamsyah[4]

*[1]School of Electrical Engineering & Informatics, Institut Teknologi Bandung, Bandung, Indonesia
titowaluyo@yahoo.com
[2]School of Electrical Engineering & Informatics, Institut Teknologi Bandung, Bandung, Indonesia
br@paume.itb.ac.id
[3]School of Electrical Engineering & Informatics, Institut Teknologi Bandung, Bandung, Indonesia
kuspriyanto@yahoo.com
[4]Algebra Research Group, Faculty of Mathematics and Natural Sciences, Institut Teknologi Bandung, Bandung, Indonesia
ntan@math.itb.ac.id

Abstract: In this paper, we propose a new metrics for predicting network security level. The proposed metrics are based on the existence of vulnerabilities in the network. The proposed metrics are Non Exploited Vulnerability Percentage (NEVP) metric, Non Vulnerable Host Percentage (NVHP) metric and Coefficient of Network Security Level (CNSL) metric. These metrics can be used to predict the security level of a networks. Formulation of the proposed metrics also explained and equipped with a clear definition. In the simulation chapter we provide a simulation results in the form of data table and two dimension graphs. These graphs are two dimension graphs consist of metrics variable and network size as x-axis and y-axis respectively. Analysis of simulation results and future works are also provided at the end part of this paper.

Keywords: Network Security Level, Metrics, Network Evaluation, Non Exploited Vulnerability, Non Vulnerable Host.

INTRODUCTION

Network Security is very important for every organization. The network with weak security have a high risk for being attacked by an attacker. This attack by an attacker will cause a security incidents. Security incidents will cause losses for organizations include loss data, data deleted or server malfunction. Security incidents can also cause loss of reputation and loss of good outsourcing relations. Thus, organizations should consider security as one of the main parameter establishing a new business to reduce these losses.

When defending an isolated network with critical resources, some vulnerabilities may seem to be insignificant. Attackers, however, can often infiltrate a seemingly well-guarded network using multi-step attacks by exploiting sequences of related vulnerabilities. Attack graphs can reveal such potential threats by enumerating all possible sequences attackers can exploit.

Each network can be regarded as a collection of systems that provide various services to its clients or users. When considering security, the measurement of security metrics must be able to produce a value and expressed as real number or percentage.

In this paper, we present a new metrics for predicting network security level based on the existence of vulnerability in the network. The first metric is Non Exploited Vulnerability Percentage (NEVP) metric, the second metric is Non Vulnerable Host Percentage (NVHP) metric and the third metric is Coefficient of Network Security Level (CNSL) metric. These metrics are explained in Sect. III. We build a definitions regarding our proposed metrics and provide a motivating examples of our metrics.

The organization of the paper is as follows. First, we discuss background and previous works in Sect. II. Then, we discuss the proposed metrics in Sect. III. A motivating examples of our security metrics provided Sect. IV. We present a simulation results in Sect V. In Sect. VI we give a conclusion for our research project.

BACKGROUND AND PREVIOUS WORKS

One of the important step in securing a network is predicting a level of network security. This step can help network administrator to modify network configurations and to choose countermeasures in order to improve security. In this work, we design a network security metrics which can be used to predict a level of network security. We propose a simple and applicable metrics to predict a level of network security. These metrics is built based on the criteria of good metric as explain in [1].

A metric is a consistent standard for measurement. A good metric should be

a. Consistently measured, without subjective criteria.
b. Cheap to gather, preferably in an automated way.
c. Expressed as a cardinal number or percentage, not with qualitative labels like “high,” “medium,” and “low”.
d. Expressed using at least one unit of measure, such as “defects,” “hours,” or “dollars”.
e. A good metric should also ideally be contextually specific—relevant enough to decision-makers so that they can take action.

More explanation about these criteria can be found in [1]. In the next paragraph, we present a previous work related to metrics for predicting or evaluating a network security.

Network Compromise Percentage (NCP) is defined as a percentage of hosts in network which accessed by attacker using user or administrator access level [2].

Lippmann et al. [2] focus on using NetSPA to verify the security of existing networks and, if necessary, create a prioritized list of recommendations for system administrators that provide the greatest improvement in network security by blocking the most destructive attack paths first.

Attack Resistance metric is proposed in [3]. Wang et al. [3] describe the metric at an abstract level as two composition operators with features for expressing additional constraints. It considers two concrete cases. The first case assumes the domain of attack resistance to be real number and the second case represents resistances as a set of initial security conditions. It show that the proposed metric satisfies desired properties and that it adheres to common sense. At the same time, it generalizes a previously proposed metric that is also based on attack graphs.

Attack Graph-based Probabilistic (AGP) metric is proposed in [4]. Wang et al. [4] propose an attack graph-based probabilistic metric for network security and studies its efficient computation.

In [5], Chen et al. explain that the compact attack graphs implicitly reveal the threat of sophisticated multi-step attacks by enumerating possible sequences of exploits leading to the compromising given critical resources in enterprise networks with thousands of hosts. For security analysts, the challenge is how to analyze the complex attack graphs with possible ten thousands of nodes for defending the security of network.

In [6], Ingols et al. explain that by accurately measuring risk for enterprise networks, attack graphs allow network defenders to understand the most critical threats and select the most effective countermeasures. Their work describe a substantial enhancements to the NetSPA attack graph system required to model additional present-day threats (zero-day exploits and client-side attacks) and countermeasures (intrusion prevention systems, proxy firewalls, personal firewalls, and host-based vulnerability scans).

In [7], Patel proposed a different method for clustering intrusion alerts. Sequences of intrusion alerts are prepared by dividing all alerts according to specified time interval. The alert sequences are considered as temporal attack graphs. The sequences are clustered using graph clustering technique, which considers similarity in sequences as a factor to determine closeness of sequences. The suggested approach combines the concept of attack graphs and clustering on sequences of alerts using graph clustering technique.

In [8], Homer et al. explain that various tools exist to analyze enterprise network systems and to produce attack graphs detailing how attackers might penetrate into the system. These attack graphs, however, are often complex and difficult to comprehend fully, and a human user may find it problematic to reach appropriate configuration decisions. Their research presents methodologies that can automatically identify portions of an attack graph that do not help a user to understand the core security problems and so can be trimmed and automatically group similar attack steps as virtual nodes in a model of the network topology, to immediately increase the understandability of the data.

In [9], Ahmed et al. explain that evaluation of network security is an essential step in securing any network. In [9], Ahmed et al. propose a novel security metric framework that identifies and quantifies objectively the most significant security risk factors, which include existing vulnerabilities, historical trend of vulnerability of the remotely accessible services, prediction of potential vulnerabilities for any general network service and their estimated severity and finally policy resistance to attack propagation within the network.

METRICS PROPOSED

Based on the criteria of good metrics and previous works on network security metrics as explained in section 2, we develop a new network security metrics based on network vulnerability. These vulnerabilities are deployed on attack graph so that our proposed metrics is based on attack graph. The proposed metrics explained in the next paragraphs.

The value of Non Exploited Vulnerability Percentage (NEVP) metric can be obtained by using equation 1.

$$\mathrm{NEVP} = \begin{cases} 100\% \text{ for } \mathrm{v} = 0 \\ \frac{v_{ne}}{v} * 100\% \text{ for } 0 < v \le \mathrm{v}_{\max} \end{cases} \quad (1)$$

where v = vulnerability on network
v_{ne} = non exploited vulnerability on network
$\mathrm{v}_{\max}$ = maximum vulnerability on network.

NEVP metric defines how many percent non exploited vulnerability on a network exist. The idea behind this metric is that the more non exploited vulnerability on a network exist the more secure the network.

The value of Non Vulnerable Host Percentage (NVHP) metric can be obtained by using equation 2.

$$\mathrm{NVHP} = \frac{\mathrm{h_{nv}}}{\mathrm{h_t}} * 100\% \quad (2)$$

where h_{nv} = number of non vulnerable host on network
h_{t} = number of host on network.

NVHP metric defines how many percent non vulnerable host on a network exist. The idea behind this metric is that the security of network increase if a number of non vulnerable host on a network increase.

NEVP metric and NVHP metric, calculated from network configuration using the formula

$$\mathrm{NEVP} = \begin{cases} 100\% \text{ for } \mathrm{v} = 0 \\ \frac{v_{ne}}{v} * 100\% \text{ for } 0 < v \le \mathrm{v}_{\max} \end{cases} \text{ and}$$

$$\mathrm{NVHP} = \frac{\mathrm{h_{nv}}}{\mathrm{h_t}} * 100\%$$

where v = vulnerability on network
v_{ne} = non exploited vulnerability on network
h_{nv} = number of non vulnerable host on network
h_{t} = number of host on network
$\mathrm{v}_{\max}$ = maximum vulnerability on network,

have minimum value 0% and maximum value 100%.

We define a Coefficient of Network Security Level (CNSL) as follow

$$\text{CNSL} = \frac{CNEVP+CNVHP}{2} \quad (3)$$

where CNEVP = Converted Non Exploited Vulneraility Percentage, and
CNVHP = Converted Non Vulnerable Host Percentage.

CNSL have minimum value 0 and maximum value 1.

The values of CNEVP and CNVHP have values between 0 (converted from 0%) and 1 (converted from 100%).

MOTIVATING EXAMPLES

We provide two examples of attack graphs. These attack graphs are derived from network configuration of hosts. In figure 1 present the attack graph derived from five hosts on the network. Hosts are represented by nodes h1, h2, h3 and Target. Exploits are represented by edges e1, e2, e3, e4 and e5.

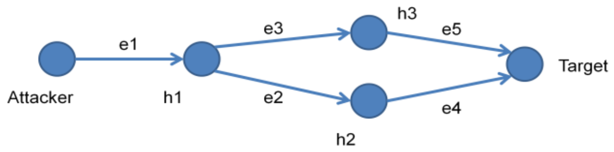

Figure 1. Example of attack graph I

In real networks, the vulnerabilities at hosts can be determined by using Nessus software. The Non Exploited Vulnerability at host can be determined using Intrusion Detection System (IDS). In this work, vulnerabilities at hosts is generated by a computer program. NEVP (Non Exploited Vulnerability Percentage) metric dan NVHP (Non Vulnerable Host Percentage) metric is obtained using equation 1 and equation 2.

Other example of attack graph is MP (Multiple Prerequisites) graph as describes in [10] can be seen in Figure 2. Hosts are represented by nodes A, B, C, D, E and F. Vulnerability are represented by nodes V_B, V_C, V_D, V_E and V_F.

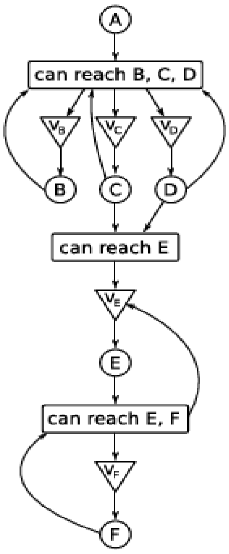

Figure 2. Example of attack graph II (Multiple Prerequisite Graph) [10]

The NVHP metric and the NEVP metric from attack graph in Figure 1 and Figure 2 are reached by equation 1 and equation 2.

SIMULATION RESULTS AND DISCUSSION

We conducted an experiment to predict the level of network security according to Equation 1, Equation 2 and Equation 3 with the definition that if network A has a higher CNSL value than CNSL value of network B, then network A is predicted more secure than network B.

Simulation results can be seen in Table 1. Table 1 present that the value of proposed metrics is between 0% and 100% as stated in the definition of these metrics.

Tabel I. Simulation Result for NEVP, NVHP and CNSL Values

Node	Normal Condition		Maximum Vulnerability		
	NEVP	NVHP	NEVP	NVHP	CNSL
10	0.80	0.50	0.00	0.00	0.65
20	0.60	0.50	0.00	0.00	0.55
30	0.27	0.63	0.50	0.00	0.45
40	0.22	0.55	0.95	0.00	0.39
50	0.81	0.48	0.56	0.00	0.64
60	0.32	0.48	0.98	0.00	0.40
70	0.19	0.54	0.40	0.00	0.37
80	0.76	0.44	0.23	0.00	0.60
90	0.78	0.59	0.09	0.00	0.69
100	0.68	0.56	0.98	0.00	0.62

In our experiment, we generate network vulnerability data then compute the NEVP metric, NVHP metric and CNSL metric of the network. We varied network size include 10 hosts, 20 hosts, 30 hosts, …, 100 hosts. The graph in Figure 3 presents the results of this simulation experiment for NEVP metric in normal condition, that is the number of vulnerability on network is between zero vulnerability case and maximum vulnerability case.

The graph in Figure 3 presents the results of this simulation experiment for NEVP metric in normal condition.

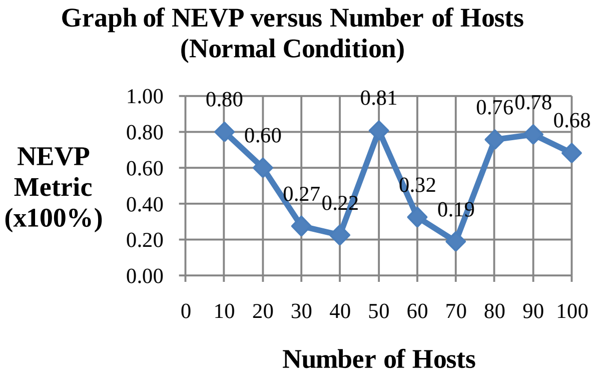

Figure 3. Graph of NEVP Metric versus Number of Hosts in Normal Condition

The graph in Figure 4 presents the results of this simulation experiment for NVHP metric in normal condition.

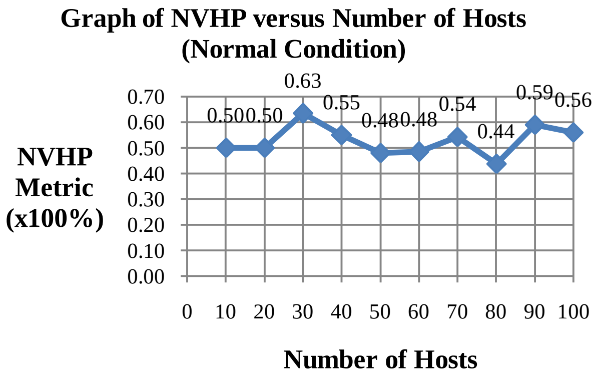

Figure 4. Graph of NVHP Metric versus Number of Hosts in Normal Condition

The graph in Figure 5 presents the results of this simulation experiment for CNSL metric in normal condition.

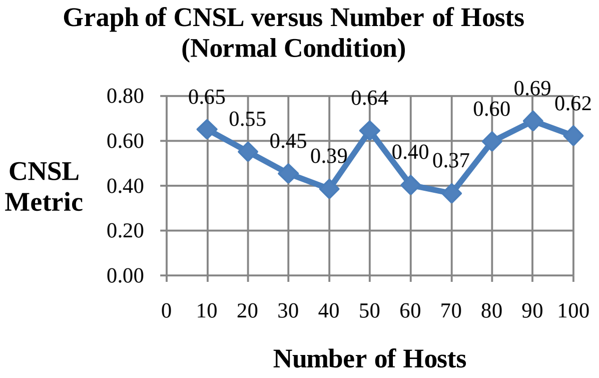

Figure 5. Graph of CNSL Metric versus Number of Hosts in Normal Condition

This simulation experiment is support and agree with the definition of our proposed metrics. Our metrics will applicable for a higher network size because it have a linear computational complexity.

CONCLUSION

In this paper, we propose a metrics to predict a level of network security. Our metrics are based on the existence of vulnerabilities on the network. We also present the graphs in coordinate x and y to show that the value of our proposed metrics have value between 0 and 1 as stated in the definition. CNSL metric can be used to predict a level of network security from a network configuration with various size.

Our experiments provide very promising results regarding our metrics. The results from our simulation is fulfil the definition of metrics as stated in Equation 1, Equation 2 and Equation 3.

We will develop the multiple security metrics including our proposed metrics which can be used to evaluate a network thoroughly in the future work.

REFERENCES

[1] A. Jaquith, Security metrics: Replacing Fear, Uncertainty, and Doubt, Pearson Education, Inc. 2007: 22.

[2] Lippmann R, Ingols K, Scott C, Piwowarski, Kratkiewicz K, Artz M, Cunningham, R. Validating and restoring defense in depth using attack graphs. Military Communications Conference, October 2006.

[3] Wang L, Singhal A, Jajodia S. Measuring overall security of network configurations using attack graphs. Data and Applications Security XXI, vol. 4602. 2007: 98–112.

[4] Wang L, Islam T, Long T, Singhal A, Jajodia S. An attack graph-based probabilistic security metric. DAS 2008, LNCS 5094. 2008: 283–296.

[5] Chen F, Liu A, Zhang Y, Su J. A Scalable Approach to Analyzing Network Security using Compact Attack Graph. JOURNAL OF NETWORKS, VOL. 5, NO. 5. 2010: 543-555.

[6] Ingols K, Chu M, Lippmann R, Webster S, Boyer S. Modeling Modern Network Attacks and Countermeasures Using Attack Graphs. Annual Computer Security Applications Conference (ACSAC) 25th. 2009.

[7] Patel H. Intrusion Alerts Analysis Using Attack Graphs and Clustering. Master Thesis. San Jose. San Jose State University; 2009.

[8] Homer J, Varikuti A, Ou X, McQueen M. A. Improving Attack Graph Visualization Through Data Reduction and Attack Grouping. Workshop on Visualization for Computer Security (VizSEC). 2008.

[9] Ahmed MS, Al-Shaer E, Khan E. A novel quantitative approach for measuring network security. Proceedings of IEEE INFO COM. 2008.

[10] Ingols K, Lippmann R, Piwowarski K. Practical Attack Graph Generation for Network Defense. In 22nd Annual Computer Security Applications Conference (ACSAC). Miami Beach. Florida. December 2006.

SHORT BIODATA OF ALL THE AUTHORS

Tito Waluyo Purboyo is currently a Ph.D. student at Institut Teknologi Bandung since August 2010. He received his Master's degree in mathematics from Institut Teknologi Bandung (2009). He is currently a research assistant at Department of Computer Engineering, School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia. His research interests include security, cryptography, physics and mathematics.

Budi Rahardjo is a teacher, lecturer, enterpreneur, writer, expert in IT security. His research interests include IT Security, including network security and application security, cryptography, high performance computing, impact of Information Technology (IT), Digital Entertainment. He received his M.Sc. (1990) and Ph.D. (1997) in Electrical Engineering from University of Manitoba, Winnipeg, Canada. Jury of various competitions/awards related to information technology and telecommunication, such as Warta Ekonomi e-Government awards (4 times), XL writing contest (3 times), and Diknas e-Education award. He is a founder of Digital Entertainment.

Digital Beat Store, the first digital music legal store in Indonesia. He has also been a consultant to industry.

Kuspriyanto is currently a Professor of Computer Engineering at Institut Teknologi Bandung. He received his DEA in Automatic System (1979) from USTL France and Ph.D. in Automatic System (1981) from the same university. He is working as a lecturer in Computer Engineering Department, School of Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia. His field of interests include network security, neural network, genetic algorithm, robotics, real time system etc.

Intan Muchtadi-Alamsyah is currently a lecturer at Department of Mathematics, Institut Teknologi Bandung and Head of Indonesian Algebraic Society. She received her DEA (Master) Méthodes Algebriques (2000) from Université de Picardie (UPJV), Amiens, France and Ph.D. in Mathematics (2004) from the same university. His research interests include: ring and module theory, representation theory of rings and algebras, homological algebra, Abelian categories, in particular derived categories and triangulated categories, and the use of algebraic structures in cryptography, bioinformatics etc.