New Non Path Metrics for Evaluating Network Security Based on Vulnerability

Tito Waluyo Purboyo[1] and Kuspriyanto[2]

[1,2] School of Electrical Engineering & Informatics, Institut Teknologi Bandung
Jl. Ganesha 10 Bandung 40132, Indonesia

Abstract

In this paper, we propose a new and simple metrics for evaluating network security. The proposed metrics are based on the existence of network vulnerabilities in the network. The proposed metrics are different with our previous metrics proposed in [11]. Exploited Vulnerability Percentage (EVP) metric, Vulnerable Host Percentage (VHP) metric and Density of Network Vulnerability (DNV) metric can be used to evaluate the security of a given network quickly because the calculation is not accompanied by path analysis. In the simulation section we provide a table of simulation results and two dimensional graphs in Cartesian coordinates. Analysis of simulation results and future works are also provided at the end part of this paper.

Keywords: *Network Security, Metrics, Network Evaluation, Exploited Vulnerability, Vulnerable Host, Vulnerability Density.*

1. Introduction

The world is becoming more interconnected with the emergence of internet and new network technologies. There is a large amount of personal information, commercial, military, and government on the network infrastructure around the world. Network security is important because intellectual property can be easily obtained via the internet.

Network security is vital to any organization. A network with weak security has high risk for attack by the attacker. The attack by the attacker will cause a security incident. Security incidents will cause harm to the organization, including lost data, deleted data or damage the server. Security incidents can also cause loss of reputation and loss of good outsourcing relationship. Thus, organizations should consider security as one of the main parameters to reduce this loss to build a new business.

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 evaluating network security based on the existence of vulnerability in the network. These metrics are Exploited Vulnerability Percentage (EVP) metric and Vulnerable Host Percentage (VHP) metric and Density of Network Vulnerability (DNV) metric. We discuss these metrics in Sect. III. We give a definition of our proposed metrics and provide a simulation study.

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. Motivating examples are given in Sect. IV. We present a simulation results in Sect. V. Conclusion and future works are given in Sect. VI.

2. Background and Previous Work

Security metrics can be categorizing as non path security metrics and path security metrics [7]. Non path analysis does not take into account the properties of attack paths which attackers must consider to follow. While path analysis does take into account the properties of attack paths. The example of non path analysis metrics are NCP metric [2] and Weakest Adversary metric [10]. In this paper we concern with non path analysis security metrics.

The NCP metric is a security metric that Lippmann et al. proposed in [2]. This metric indicates the percentage of network assets an attacker can compromise. While the definition of compromise can be flexible to suit one's situation, Lippmann et al. defined a host compromise as the attacker attaining user-level or administrator-level access on a host. The more compromised machines, the higher the NCP value. Hence, the security engineer's goal is to minimize the NCP metric.

Pamula et al. propose the Weakest Adversary metric in [10]. The Weakest Adversary metric is similar to the

Shortest Path metric in that it attempts to express the security of the network in terms of the weakest part of the network. The intuition of the metric is that one's network is no stronger than the weakest adversary, that is, the adversary with the weakest set of capabilities. Weakness of an adversary is correlated with the initial attributes of an attack graph. Each attack graph has some set of initial attributes that allows for the realization of a security policy violation. If comparing the security of two networks, the network requiring a weaker set of initial attributes to compromise the network is deemed less secure. A set of initial attributes is deemed weaker than another set of initial attributes if it is a proper subset of the other set of initial attributes. Alternative relations could be defined for determining which of two networks has a weaker set of initial conditions.

Our metrics are developed based on the points of view as describe in the following explanation.

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 discuss some metrics for evaluating 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] described a tool named NetSPA (Network Security and Planning Architecture) which can be used to verify and, if necessary, to provide suggestions to restore defense in depth for large enterprise networks. It provides a comprehensive solution that is not currently available due to the limitations of current security tools. For example Network vulnerability scanners, such as Nessus, discover hundreds or thousands of vulnerabilities on even small networks but do not indicate which of these enable an attacker to progress through a network to reach critical resources. A firewall rule set evaluator identifies common misconfiguration, such as rules permitting arbitrary inbound traffic to a common server port, but again does not indicate which rules permit an attacker to reach critical resources.

Attack Resistance metric is proposed in [3]. Wang et al. [3] described the metric at an abstract level as two composition operators with features for expressing additional constraints. They consider 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 shows 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] proposed an attack graph-based probabilistic metric for network security and studies its efficient computation.

In [5], Chen et al. explained 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. explained 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. Ingols et al. [6] described 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 [8], Homer et al. explained that there are a 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. Homer et al. [8] presented a methodology 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. explained that evaluation of network security is an essential step in securing any network. This evaluation can help security professionals in making optimal decisions about how to design security countermeasures, to choose between alternative security architectures, and to systematically modify security configurations in order to improve security. However, the security of a network depends on a number of dynamically changing factors such as emergence of new vulnerabilities and threats, policy structure and network traffic. Identifying, quantifying and validating these factors using security metrics is a major challenge in this area. 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.

3. The Proposed Metrics

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

Exploited Vulnerability Percentage (EVP) metric can be obtained by using the formula as stated in equation 1.

$$EVP = \begin{cases} 0\% \text{ for } v = 0 \\ \frac{v_e}{v} * 100\% \text{ for } 0 < v \leq v_{max} \end{cases} \quad (1)$$

where v = vulnerability on network
v_e = exploited vulnerability on network
v_{max} = maximum vulnerability on network.

EVP metric defines how many percent of exploited vulnerability exist on a network. The idea behind this metric is that if an exploited vulnerability on a network increase then the network is become less secure.

Vulnerable Host Percentage (VHP) metric can be obtained by using the formula as stated in equation 2.

$$VHP = \frac{h_v}{h_t} * 100\% \quad (2)$$

where h_v = number of vulnerable host on network
h_t = number of host on network.

VHP metric defines how many percent of vulnerable host exist on a network. The idea behind this metric is as follow. If vulnerable hosts on a network increase, the network becomes less secure.

Density of Network Vulnerability (DNV) metric can be obtained by using the formula as stated in equation 3.

$$DNV = \frac{v_t}{h_t} \quad (3)$$

where v_t = number of vulnerability on network
h_t = number of host on network.

DNV metric represent the density of vulnerability on network, i.e. equivalent with the average number of vulnerability per host. The idea behind this metric is as follow. If a vulnerability on a network increase, then the attacker has more choices to exploit much vulnerability. It's mean that network become less secure.

EVP metric and VHP metric calculated from network configuration have minimum value 0% and maximum value 100% and can be calculated with the formulas

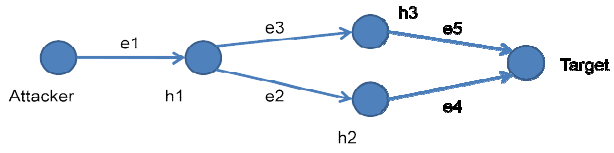
$$EVP = \begin{cases} 0\% \text{ for } v = 0 \\ \frac{v_e}{v} * 100\% \text{ for } 0 < v \leq v_{max} \end{cases} \text{ and}$$

$$VHP = \frac{h_v}{h_t} * 100\%$$

where v = vulnerability on network
v_e = exploited vulnerability on network
h_v = number of vulnerable host on network
h_t = number of host on network
v_{max} = maximum vulnerability on network.

4. A Motivating Examples

We provide two examples of an attack graph. These attack graphs are derived from network configuration of hosts. In figure 1 is presented 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.



EVP = (4/4) x 100% = 100%
VHP = (4/4) x 100% = 100%

Fig. 1 Example of attack graph I

In a real network, the vulnerabilities at hosts can be determined by using Nessus software. The Exploited Vulnerabilities at host are determined using Intrusion Detection System (IDS). In this work, vulnerabilities at hosts are generated by a computer program. EVP (Exploited Vulnerability Percentage) metric and VHP (Vulnerable Host Percentage) metric are obtained using equation 1 and equation 2.

Other example of attack graph and the value of VHP metric and EVP metric can be seen in Figure 2. Hosts are represented by nodes h1, h2, h3, h4 and Target. Exploits are represented by edges e1, e2, e3, e4, e5 and e6.

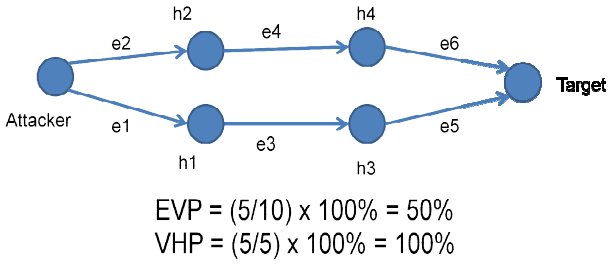


Fig. 2 Example of attack graph II

The VHP metric from attack graph in Figure 1 and Figure 2 have the same value. Because EVP metric which is calculated from attack graph II is less than EVP metric which is calculated from attack graph II, we can predict that network II is more secure than network I.

5. Simulation Results

We conducted an experiment to evaluate the network security according to equation 1, equation 2 and equation 3.

Table 1: Simulation Result for EVP and VHP Values

Node	Normal Condition			Maximum Vulnerability		
	EVP	VHP	DNV	EVP	VHP	DNV
10	0.25	0.10	3.30	0.70	1.00	6.90
20	0.73	0.30	5.85	0.55	1.00	8.40
30	0.71	0.33	3.40	0.47	1.00	8.00
40	0.77	0.23	3.58	0.63	1.00	6.93
50	0.76	0.38	2.88	0.58	1.00	8.82
60	0.79	0.50	4.52	0.55	1.00	7.93
70	0.71	0.54	4.41	0.51	1.00	7.37
80	0.66	0.51	3.86	0.45	1.00	8.69
90	0.81	0.50	4.37	0.67	1.00	7.61
100	0.90	0.45	3.69	0.37	1.00	8.23

Simulation results can be seen in Table 1. We present in Table 1 that the values of EVP and VHP metrics is between 0% and 100% as stated in the definition as stated in equation 1 and equation 2. While the DNV metric value represent the average number of vulnerabilities per host.

In our experiment, we generate a network vulnerabilities data then compute the EVP, VHP and DNV metrics from the data. 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 EVP metric in normal condition, which is the number of vulnerability on network, is between zero vulnerability case and maximum vulnerability case.

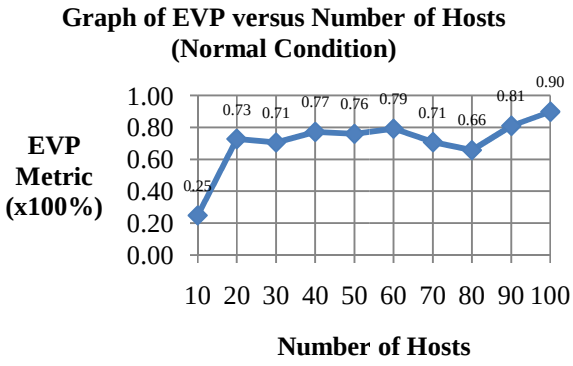


Fig. 3 Graph of EVP versus Number of Hosts in Normal Condition

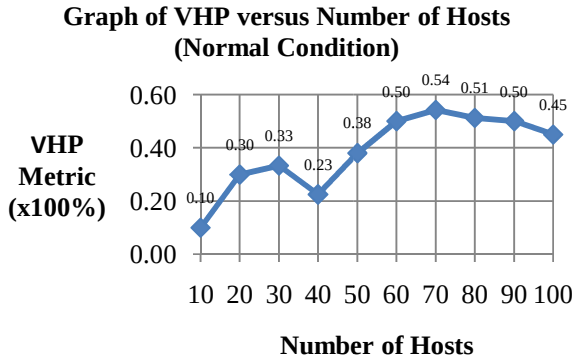


Fig. 4 Graph of VHP versus Number of Hosts in Normal Condition

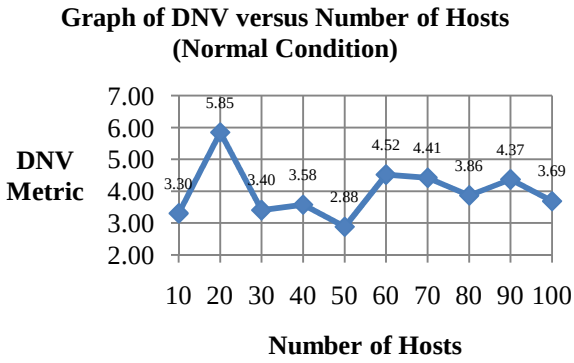


Fig. 5 Graph of DNV versus Number of Hosts in Normal Condition

The calculation results of our proposed metrics are presented in Fig. 3, Fig. 4 and Fig. 5. Figure 3 represents the simulation result for EVP metric in normal condition. The graph in Figure 4 presents the results of this simulation experiment for VHP metric in normal condition. The graph in Figure 5 presents the results of this simulation experiment for DNV metric in normal condition.

These simulation experiments is support and agree with the definition of our metrics as stated in chapter 3.

6. Conclusions and Future Works

In this paper, we propose a metrics to evaluate network security. These metrics are based on the existence of vulnerabilities on the network. We further present the arithmetic equation for computing EVP, VHP and DNV metrics. We also present the graphs of each metric versus number of hosts in Cartesian coordinate.

Our experiment provides that the computation of our proposed metrics is very simple and fast. The results of our simulation are fulfills the definition and the arithmetic formula as stated in equation 1, equation 2 and equation 3.

There are many open problems in the security metrics research area as stated in [12]. In the future works, we will provide the multiple security metrics including our proposed metrics which can be used to evaluate a network security thoroughly. We will develop a network security metrics based on path analysis in the future. We will also try to develop the network security metrics based on attack graph and its relation with Eigen pair [13] and other properties of a graph.

Acknowledgment

This research is supported by the LPPM Institut Teknologi Bandung, Research Grant: 0281/I1.C07/PL/2012.

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. Proceeding of Data and Application Security. 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] Idika N, Bhargava B. Extending Attack Graph-Based Security Metrics and Aggregating Their Application. IEEE Transactions on Dependable and Secure Computing, Vol. 9, No. 1, January/February 2012.
[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] Pamula J, Jajodia S, Ammann P, and Swarup V. A Weakest-Adversary Security Metric for Network Configuration Security Analysis. Proc. Second ACM Workshop Quality of Protection, pp. 31-38, 2006.
[11] T. W. Purboyo, B. Rahardjo, Kuspriyanto, I. M. Alamsyah. A New Metrics for Predicting Network Security Level. Journal of Global Research in Computer Science, Volume 3, No. 3, March 2012.
[12] T. W. Purboyo, B. Rahardjo, Kuspriyanto. Security Metrics: A Brief Survey. 2011 International Conference on Instrumentation, Communication, Information Technology and Biomedical Engineering, Bandung, Indonesia, 8-9 November 2011.
[13] Irawati, T. W. Purboyo. Developing Computer Program for Computing Eigen pairs of 2x2 Matrices and 3x3 Upper Triangular Matrices Using The Simple Algorithm. Far East Journal of Mathematical Sciences (FJMS), Volume 56, Issue 2, p. 185-200, September 2011.

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.

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 fields of interests include network security, neural network, genetic algorithm, robotics, real time system etc.