International Journal of
Science and Engineering Investigations vol. 1, issue 7, August 2012
ISSN: 2251-8843

Attack Graph Based Security Metrics: State of the Art

Tito Waluyo Purboyo[1], Kuspriyanto[2]
[1,2]School of Electrical Engineering and Informatics, Institute Technology Bandung, Indonesia
([1]titowaluyo@yahoo.com, [2]kuspriyanto@yahoo.com)

***Abstract*-** In this paper, we discussed the development of Attack Graph-Based Security Metrics that will be used to evaluate the security of a network. Attack Graph-Based Security Metrics recently used simultaneously to form a Multiple Attack Graph-Based Security Metrics. Furthermore, Multiple Attack Graph-Based Security Metrics were used to evaluate the two networks so it can be inferred which network is more secure than other one.

***Keywords*-** *Network Security Metrics, Attack Graph, Network Hardening.*

I. INTRODUCTION

Security incidents can cause very large losses for a company and not just direct losses, but also the loss of reputation and outsourcing relationships. Therefore, an organization should consider security as one of the main parameters in building a new business to reduce these losses. Security should be considered at the earliest stages of design to define the architecture to be selected. To do that the company should implement a quantitative security evaluation of various design alternatives. The results of this evaluation will also demonstrate the safety conditions (security state) of a system to a security manager or outsourcing partner, helping to establish the installation of a new security control, estimate the expected risk for a particular service.

One type of security metrics is closely related to the analysis of an organization's security is an attack graph-based security metrics. Attack graph is an abstraction that states how an attacker can violate a security policy by exploiting the interdependence between the various vulnerabilities.

In this paper will also be presented how the process to get the metrics that will be submitted as a novelty. The new attack graph-based security metrics is generated based on the criteria of determination a good metrics. Some of the metrics that have been previously generated (e.g. Network Compromise Percentage Metric) also inspired how the new attack graph-based security metrics can be found.

Multiple attack graph-based security metrics is just the combination of different metrics. The combination of attack graph-based security metrics chosen are based on simplicity of form and ease of analyzing these metrics.

In this paper also conducted research on how to determine an evaluation of the security of a network. Evaluation of network security using multiple attack graph-based security metrics is relatively new. In addition to security evaluation of a network, it also can be used for evaluation of two or more networks so the network security of the two network configurations can be compared.

In the final part of this research, we will improve the security of the network by using the principle of eliminating or reducing the vulnerability on the network. The principle of elimination or reduction of vulnerability is will be done in future work using linear programming optimization. Any kind of countermeasures to eliminate the vulnerability requires a certain fee. Based on the various types of these countermeasures, we will select the most optimal countermeasures without exceeding available funds. So problem solved is the problem of priority to select the most optimal countermeasures based on barrier of the funds available to make improvements to network security hardening.

II. AN OVERVIEW OF SECURITY METRICS

The definition of metrics according to [6] is a value that facilitates decision making and is derived from the measurements.

According to [1], the metrics are the result while measurement is an activity. Measurement is an implementation of the activities of observation and data collection in an effort to gain a practical view of what is being attempted to be understood. The collection of data security is very important to implement an effective safety program. However, if no context to the data and ideas on the reasons why the data was collected and for what purpose the data is collected, the limitations in describing such measurements are limited to the terms terabytes of log data and the volume occupied by shelves auditor's report.

In [2], the standard metric is consistent for a given measurement. Good metrics should be measured consistently, cheap to get it, otherwise the cardinal number or percentage, expressed by at least one unit of measurement, specific contextual (relevant enough so that decision makers can take a decision).

Idika in [6] states that the security metrics are the values resulting from the measurement of an entity attributes (which can be identified) that affect physical security, personnel, IT or operational.

Krautsevich in [11] states that the security metrics are the tools for providing correct and current information about the state of the security. This information is essential for managing security efficiently.

Security Metrics can be classified into several categories [6], i.e. Return on investment (ROI) metrics, Resiliency metrics and Compliance metrics.

ROI metrics measure monetary gain through the resources of an organization dedicated to the security control.

Resiliency metrics measure the ability of an organization to maintain acceptable service in the presence of an attack or failure.

Compliance metrics measure how well an organization to comply with the rules or standards. In [8] discussed the level of resistance of a software product against malware (malicious software). Analysis was performed on software architecture. This analysis can be done based on the results of a software design process, because it can be used in the early stages of development.

The dissertation [5] has a primary focus on the collection of security indicators for a service using business process models and enterprise and not reviewing the evaluation of a company simultaneously as usual approach. Furthermore, the existing approaches are based on the selection of security controls at the time of choosing security architecture. This approach is more suitable for a Service Oriented Architecture (SOA) where there are many possible alternative designs.

In [7] explained that the effectiveness of security measures and the possibility of software vulnerability discovery will be instrumental in improving security. One technique proposed for understanding better security software is by modeling the vulnerability discovery.

In [10] discussed that if at the time of attacking a software system to be just as difficult as finding a vulnerability to be exploited, then the security forces to be equivalent to the market price of such vulnerability. In the dissertation [10] it is shown that the security forces can be measured based on market conditions, how it is measured can be applied to create a model that can predict the security risk faced by the system, and how the power of the market can also be removed to improve the security forces through the software development process. In short, the dissertation is presented as-needed basis in quantitative and comprehensive approach to improving the security forces and reduce security risk.

Network security can be analogous to a security fortress. In Figure 1 the following can be seen a tree diagram that shows how the walls of a fortress may be penetrated by an attacker [10].

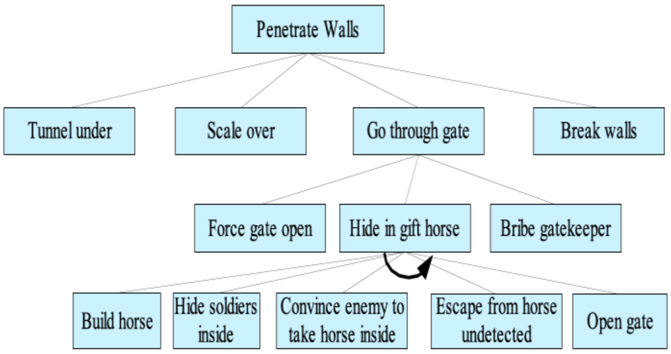

Figure 1. Network Security Analogy with Fortress Security

In the dissertation [9], Liu explained that the development of intrusion activity very quickly lead to the definition and evaluation of software safety requirements to be an important aspect of software development services. Today has been widely accepted fact in software engineering that security concerns, as well as other quality concerns, should be considered in the early stages of the software development process. Risk analysis for software security architecture is still very dependent on human expertise. He proposes a framework for quantitative analysis of security architecture for service-oriented software systems.

In [11], Krautsevich et. al. explained that the security metrics are tools to provide correct and current information about the state of security. This information is essential for managing security efficiently. Although a number of security metrics have been proposed, we still need a reliable way to assess safety. The first thing to note, we do not have a definition that is not ambiguous and widely accepted that defines what it means to a more secure system than other systems. Without this knowledge, we cannot show that a metric really measures security. Secondly, there is no formal model that applies universally to all the metrics that can be used to perform a thorough analysis. In the paper [11] is described how the researchers define the relationship "more secure" and filed a formal model to describe and analyze the basis of a security metrics.

III. State of The Art of Attack Graph-Based Security Metrics

State of the Art of attack graph-based security metrics can be seen in Table 1. Network Compromise Percentage (NCP) is defined as the percentage of hosts on the network that can be accessed by an attacker using a user or administrator level access [12].

Attack Resistance (AR) of a network configuration is defined as the composition of individual exploits measurements [13]. Attack Graph-based Probabilistic (AGP) is defined as an attack graph that has a value on any exploit or condition where the value is declared an attacker exploit the possibility of an exploit [14]. Expected Risk (ER) for a service is defined as the product of the chance of at least one of the new vulnerability will affect service on the next period and the expected value of severity vulnerability [19].

TABEL 1. State of The Art of Attack Graph-Based Security Metrics

No.	Research Title/Year	Metrics Proposed	Single/Group	Algorithm
1.	Validating (Lippmann et. al. 2006)	Network Compromise Percentage (NCP)	Single	
2.	Measuring (Wang et. al.. 2007)	Attack Resistance (AR)	Single	Breadth-first
3.	An attack graph-based (Wang et. al. 2008)	Attack Graph-based Probabilistic (AGP)	Single	Modified breadth-first search (BFS)
4.	A novel quantitative (Ahmed et. al. 2008)	Expected Risk (ER)	Single	
5.	A Scalable Approach (Chen et. al.. 2010)	Security Risk	Single	Recursive, weighted-greedy
6.	Characterizing (Idika 2010)	SP, NP, NMPL, SDPL, MoPL, MePL, K-step Capability Accumulation (KCA)	Group	Depth-first search
7.	T.W. Purboyo et. al. (2012)	SP, NMPL, MePL, EVP, VHP	Group	Depth-first search

Security Risk (SR) is defined as the metrics measured by many factors trajectory of attack, attack the track distance and the number of types of exploits in the trajectory of attack [15]. Shortest Path (SP) is defined as the shortest path attacks can be exploited by an attacker to achieve the goal. Number of Path (NP) is defined as the number of walks that are offensive attack on a graph. Normalized Mean of Path Length (NMPL) is defined as the average path length normalized attacks (divided by the number of walks of attack).

Standard Deviation of Path Length (SDPL) is defined as the standard deviation of the path length contained an attack on an attack graph. Mode of Path Length (MoPL) is defined as a mode of attack path length contained in an attack graph. Median of Path Length (MePL) is defined as the median of the attack path length contained in an attack graph. K-step Capability Accumulation (KCA) is defined as the energy gained by an attacker on the network in K steps [6]. Exploited Vulnerability Percentage (EVP) is defined as the percentage of the exploited vulnerability on the network. Vulnerable Host Percentage (VHP) is defined as the percentage of vulnerable hosts on the network.

Lippmann et. al. explained that the defense in depth is a common strategy that uses multiple layers to protect subnet supervisory control and data acquisition (Supervisory Control and Data Acquisition-SCADA) and other critical resources on enterprise networks [12].

Wang et al. [13] explained that the computer systems are facing various vulnerabilities intrusion which can be combined to achieve the purpose of the attack. To measure the security of a network system, the first thing to understand is how the vulnerability combined to produce an attack. Such understanding is possible with the composition modeling vulnerability as an attack graph.

Wang et al. explained that in order to protect important resources in a networked environment, it needed a way to quantify the possibility of multi-step attack potential to combine the various vulnerabilities. This is made possible by the attack graph. This paper proposes attack graph-based probabilistic metric for network security and research computing efficiently [14].

In [15], Chen et al. explained that the compact attack graphs implicitly indicate a threat of a multi-step attacks by trying possible sequences of exploits which led compromises significant resources in enterprise networks with thousands of hosts.

Ingols et al. explained that the measurements accurately on enterprise networks, attack graphs allow network defenders to understand the critical threats and select the most effective countermeasures [16].

In [17], Patel explained that the security of networks and information is crucial in maintaining the information infrastructure in order to remain safe. An attack graph tools to model network security vulnerability reviewing individual global perspective in which individual hosts are connected.

Homer et al. explained that the various tools that exist to analyze enterprise network systems and to produce attack graphs detailing how attackers can penetrate into the system [18].

In [19], Ahmed et. al. explained that the evaluation of network security is an essential step in securing the network. This evaluation can help security professionals in determining optimal decisions about how to design security countermeasures. Choosing alternative security architecture, and systematically modify security configurations in order to increase security.

IV. Conclusion

Developing a metrics to evaluate network and network security hardening still needs to be done. The development of these metrics can be directed to the analysis process easier and faster. The combinations of several metrics become Multiple Attack Graph-Based Security Metrics can be developed further. This combination is intended to obtain ease in implementation of network security evaluation and network security hardening.

Based on the metrics that have been proposed by previous researchers, and taking into account the criteria of good metrics, the authors propose metrics to evaluate network security which has never been proposed yet by previous researchers, namely EVP (Vulnerability Exploited Percentage) Metric and VHP (Vulnerable Host Percentage) Metric [24].

Multiple Attack Graph-Based Security Metrics recently proposed by the authors as a novelty, namely SP (Shortest Path) Metric, NMPL (Normalized Mean of Path Length) Metric, MePL (Median of Path Length) Metric, EVP (Vulnerability Exploited Percentage) Metric and VHP (Vulnerable Host Percentage) Metric.

There are many open problems in the security metrics research area as stated in [20, 23]. 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 [21] 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] L. Hayden, “IT Security Metrics,” The McGraw-Hill Companies, New York, 2010.

[2] A. Jaquith, “Security metrics : replacing fear, uncertainty, and doubt,” Pearson Education, Inc., 2007.

[3] S.M. Furnell, S. Katsikas, J. Lopez, A. Patel, “Securing Information and Communications Systems: Principles, Technologies, and Applications,” Artech House, Inc., 2008.

[4] J.M. Kizza, “A Guide to Computer Network Security,” Springer-Verlag London Limited, 2009

[5] A. Yautsiukhin, “A Framework for Quantitative Security Analysis of Complex Business Systems” PhD Dissertation, International Doctorate School in Information and Communication Technologies (DIT), University of Trento, 2009.

[6] N.C. Idika, “Characterizing and Aggregating Attack Graph-Based Security Metrics,” PhD Dissertation, Purdue University, West Lafayette, Indiana, 2010.

[7] A. Ozment, “Vulnerability Discovery & Software Security,” PhD Dissertation, University of Cambridge, 2007.

[8] H. Langweg, “Software Security Metrics for Malware Resilience,” PhD Dissertation, Bonn University, 2007.

[9] M.Y. Liu, “Quantitative Security Analysis for Service-Oriented Software Architectures,” PhD Dissertation, Department of Electrical and Computer Engineering, University of Victoria, 2008.

[10] S.E. Schechter, “Computer Security Strength & Risk: A Quantitative Approach,” PhD Dissertation, The Division of Engineering and Applied Sciences, Harvard University, 2004.

[11] L. Krautsevich, F. Martinelli, A. Yautsiukhin, “Formal approach to security metrics: What does “more secure” mean for you?,” IEEE Paper, IEEE/ASME International Conference on Mechatronic and Embedded Systems and Application, 2010.

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

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

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

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

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

[17] H. Patel, “Intrusion Alerts Analysis Using Attack Graphs and Clustering,” San Jose State University, 2009.

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

[19] M.S. Ahmed, E. Al-Shaer, E. Khan, “A novel quantitative approach for measuring network security,” Proceedings of IEEE INFO COM 2008.

[20] T.W. Purboyo, B. Rahardjo, Kuspriyanto, “Security Metrics: A Brief Survey,” Proc. of 2011 International Conference ICICI-BME, Bandung, 8-9 Nov. 2011.

[21] 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.

[22] N. Idika, B. Marshall, B. Bhargava, “Maximizing Security given a Limited Budget,” Proc. TAPIA ’09: Richard Tapia Celebration of Diversity in Computing, Apr. 2009.

[23] T.W. Purboyo, B. Rahardjo, Kuspriyanto, I.M. Detiena, “A New Metrics for Predicting Network Security Level,” Journal of Global Research in Computer Science (JGRCS), Vol. 3 No. 3 p. 68-72, March 2012.

[24] T.W. Purboyo, Kuspriyanto, “New Non Path Metrics for Evaluating Network Security Based on Vulnerability,” International Journal of Computer Science Issues, Volume 9, Issue 4, July 2012.

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.