ISSN:0975-9646

Attack Graph-Based Security Metrics and other Metrices for Producing Security to the Computer Network

Ms.Patil Priyanka Nagnath
P.G Student
M.E Computer science & Engineering,
Shriram Institute of Eng. & Technology,
Paniv, Maharashtra, India

Prof.Prakash B. Dhainje
Vice-Principal Computer science & Engineering
Shriram Institute of Eng. & Technology
Paniv, Maharashtra, India

Dr.Deshmukh Pradeep K.
Principal Computer science & Engineering
Shriram Institute of Eng. & Technology
Paniv, Maharashtra, India

Abstract-The paper suggests an approach to network attack modeling and security evaluation which is realized in advanced Security Information and Event Management (SIEM) systems. It is based on modeling of computer network and malefactors' behaviors, building attack graphs, processing current alerts for real-time adjusting of particular attack graphs, calculating different security metrics and providing security assessment procedures. Increasing inclination of people to use software systems for most of the purposes comes a major challenge for software Engineers the engineering of secure software systems. The concept of computer Security is being heavily researched and this perfectly makes sense in a world where e-commerce and e governance are becoming the norms of the day. Along with their potential for making life easier and smarter for people, these systems also carry with them the danger of insecurity. Because any software system is an outcome of some software engineering process it makes sense to incorporate security considerations during the software engineering processes. We use the attack based graph to provide the security to network. For that purpose we use the shortest path metric, the Number of Paths metric, and the Mean of Path Lengths metric are three attack graph-based security metrics that can extract security-relevant information. The Shortest Path metric and the Mean of Path Lengths metric fail in the number of ways an attacker may violate a security policy. The Number of Paths metric fails to adequately account for the attack effort associated with the attack paths. To overcome these shortcomings, we propose a complimentary suite of attack graph-based security metrics and specify an algorithm for combining the usage of these metrics.

Attack graph can provide clues for the network defender on how an attacker exploits the vulnerability on the network to achieve goals. System administrators use attack graph to determine how vulnerable their systems and to determine what security measures are used to maintain their systems. In a network of large and complex organizations, securing a network is a very challenging task. Attack graphs are very important in the effort to secure the network, because it can directly indicate the presence of vulnerabilities in network and how attackers use the vulnerabilities to implement an effective attack. In this paper, we will describe some very good algorithms can be used to generate the attack graph.

Keywords Network-level security and protection, Attack Graph.

I. INTRODUCTION

Computer network has grown both in size and complexity with the advent of Internet. It facilitates easy access to vast store of reference materials, collaborative computing, and information sharing. However, this requires a secure interconnected world of computing where confidentiality, integrity, and availability of information and resources are restored. Traditionally, security mechanism is enforced by access control and authentication. However, these security best practices do not take operating system, or network service-based or application vulnerabilities into account. With the evolution of sophisticated hacking tools, attackers exploit these vulnerabilities and can gain legitimate access to network resources, bypassing the access control and authentication policies. One tool that presents a succinct representation of different attack scenarios specific to a network is attack graph. Attack graph models service or application-based attacks and depicts all possible multi host multi-step attack scenarios that an attacker can launch to penetrate into an enterprise network. The severity associated with each attack scenario can be evaluated following some attack graph-based security metrics.

A completely secure network is one where no attacker can violate a security policy of that network. Since such a system is currently impractical, an approximation to it would be one where the attacker has extreme difficulty violating the network's security policies. Tom DE Marco stated, ―You can't control what you can't measure. This clearly states the importance of metrics in software engineering. Since quantitative methods have proved so powerful in other sciences, computer science practitioners and theoreticians have worked hard to bring similar approaches to software development.

Even though many software metrics are now available, most of the metrics have lacked a sound theoretical basis or a statistically significant experimental validation. Despite these problems, it appears that the judicious methodical application of software metrics can aid significantly in improving software quality and productivity.

Engineering of secure software systems seems to be one of the most important challenges confronted by software practitioners today and hence it is worth exploring the possibility of using metrics to aid the software engineers in this regard. An enterprise security goal is to remove all

networks and host vulnerabilities. Attacks that use existing network vulnerabilities that successfully violate a security policy, may be done with a single attack action or a series of attack actions. A series of attack actions is sometimes referred to as a chained exploit. Chained exploits leverage the interdependencies that exist among vulnerabilities to violate a network's security policy. The vulnerabilities existing in Adobe Reader and the AV scanners on the mail server and end user desktops made then chained exploit possible. The set of all chained exploits that violate a security policy, or a set of security policies, can be captured by an attack graph. Security-relevant information is extracted by using the attack graph & sometimes we use the attack graph analyses. There are two security metrics that have inspired KCA: the Shortest Path metric and the Network Compromise Percentage (NCP) metric. If the Shortest Path metric, from Phillips and Swiler, is being used under KCM-quant, then the shortest attack path in the attack graph corresponds to the path with the fewest number of edges. If KCM-quell is used, then the shortest path in the attack graph corresponds to the path that produced through arithmetic/algebraic manipulations the value considered to have the least resistance in comparison to other paths. KCA and the Shortest Path metric can be similar when using a goal-oriented attack graph. However, KCA can be applied to attack graphs with no goal states. The Shortest Path metric, on the other hand, cannot be applied to attack graphs with no goal states. Thus, KCA is more versatile in its applicability to different types of attack graphs.

When there is a goal state and the semantics of the attack graph are such that this goal state has all of the asset value in the network, the KCA metric may degenerate to the Shortest Path metric. For instance, if the attacker can reach the goal state in single step and the non-attacker nodes are of little value with respect to the target node, then using the Shortest Path metric without KCA would be sufficient for determining which of the two networks is most secure.

Security evaluation based on comprehensive simulation of malefactor's actions, construction of attack graphs and computation of different security metrics. The approach is intended for using both at design and exploitation stages of computer networks. The implemented software system is described, and the examples of experiments for analysis of network security level are considered.

For a given network, administrators require a comparative assessment of different configurations. Also, the objective of an administrator is to minimize the cost incurred while making changes to a configuration for securing the critical assets. Such what-if queries related to optimization of cost of configuration change and security values are addressed by quantification of security strengths, done by metrics. We propose different attack graph-based metrics which have been reported in the literature are presented.

II. LITERATURE SURVEY

A critical analysis of each metric is carried out to-Security metrics can be categorizing as non path security metrics and path security metrics. 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 examples of analysis metrics are NCP metric and Weakest Adversary metric. In this paper we concern with non path analysis security metrics. The NCP metric is a security metric that Lippmann et al. proposed in 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.

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.

A. Shortest Path (SP) Metric

This metric defines the security of a attack graph in terms of the shortest path from the initial security condition to the goal condition Mathematically, if G denotes an attack graph, then SP metric is given as,

$SP(G) = \min\{l(p1), l(p2), \ldots, l(pn)\}$ (1)

Where (pi) denotes the length of the ith attack path in the attack graph. Intuitively, this metric represents the minimum amount of effort an attacker needs to compromise a target.

B. Number of Paths (NP) Metric

This metric denotes the number of ways an attacker can compromise the goal conditions in an attack graph the higher the number of paths, less is the security strength of the network. That is, the attacker has more options by which he can attain the goal. Mathematically,

$NP(G) = jp1; p2; ::::pnj = n$ (2)

C. Mean Path Length Metric (MPL)

The *MPL* metric represents the expected number of exploits an attacker should execute in order to reach the goal condition in a given attack graph. It is computed by taking the arithmetic mean of all the attack path lengths in the attack graph.

III. PROPOSED SYSTEM AND DESIGEN

Attack Based Model

Attack graph combines vulnerabilities existing on different hosts to generate attack scenarios. Researchers have defined various forms of attack graphs viz. In this work, security metrics concerned only with the exploit dependency graph have been taken into account.

Essentially, an exploit-dependency graph (will be called attack graph interchangeably) consists of a number of attack paths (or, scenarios),each of which is a logical succession of exploits and conditions .Conditions in an attack graph

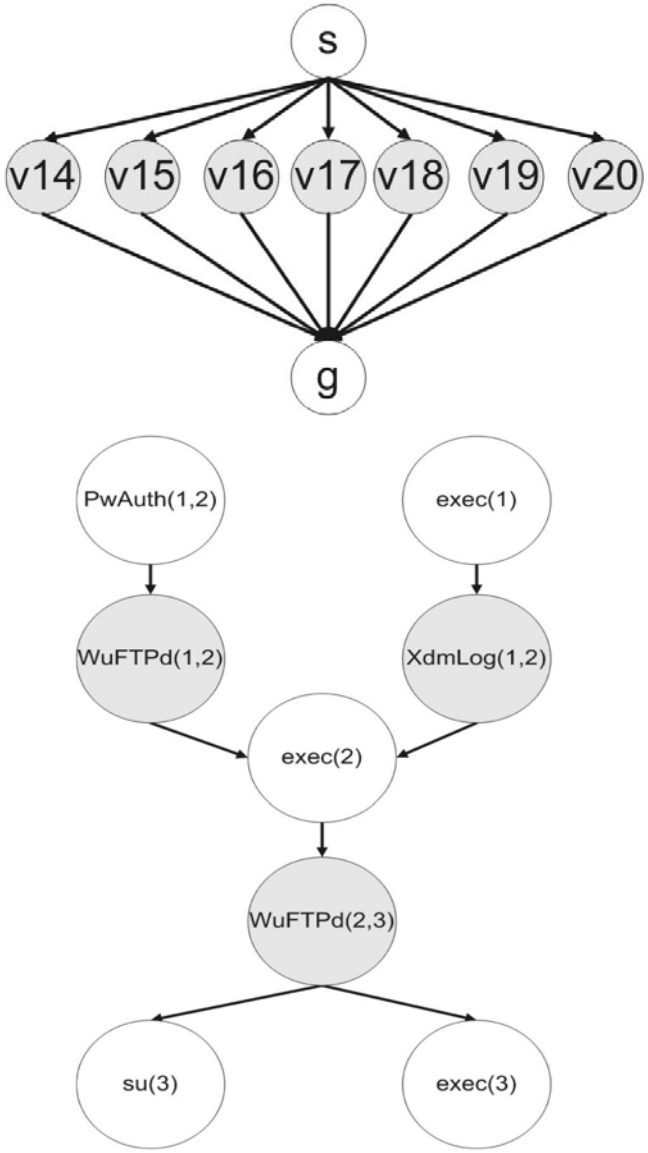

Fig. An Example Attack Graph

Fig Attack Graph Gi with vulnerabilities 14 through 20. represent different attributes of network objects, viz. hosts, network devices, etc. and includes the following.

-Platform, architecture, operating system versions of different hosts

_ Privilege levels in different hosts

_ Availability of vulnerable versions of applications

_ Network and transport level connectivity among different hosts

To generate attack graph, a set of *initial conditions* and *goal conditions* are required. Initial conditions refer to those network states which are available by default. The perspective directions in evaluating network security are simulating possible malefactor's actions, building the representation of these actions as attack graphs (trees, nets), the subsequent checking of various properties of these graphs, and determining security metrics which can explain possible ways to increase security level.

CONCLUSION

In this work we use three path-analysis attack graph-based security metrics. Attack Graph-Based Security Metrics provide security to the computers from unwanted threads.

Our future work producing more and more attack graph based security metrics which provides the security to the computer networks. Increasing the number security metrics that provide unique security-relevant information will enhance the security engineer's ability to assess a network's security and to perform network hardening. Future work also includes developing enhanced approaches for quantitatively measuring attack path complexity.

ACKNOWLEDGEMENT

The proposed system is based on IEEE Transaction paper under the title Extending Attack Graph-Based Security Metrics and Aggregating Their Application published in IEEE TRANSACTIONS ONDEPENDABLE AND SECURE COMPUTING, VOL.9,NO.1, JANUARY/FEBRUARY 2012

REFERENCES

1. SSE-CMMhttp://www.sse cmm.org/metric/metric.asp, 2010.
2. C.Weissman,"SystemSecurity Analysis/Certication Methodology and Results," Technical Report SDC SP-3728, 1973.
3. N. Idika, B. Marshall, and B.Bhargava, "Maximizing Security given a Limited Budget," Proc. TAPIA '09: Richard Tapia Celebration of Diversity in Computing, Apr. 2009.
4. R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, and R. Cunningham, "Validating and Restoring Defense in Depth Using Attack Graphs," Proc. Military Communications Conf., Oct. 2006.
5. J.Pamula, S. Jajodia, P. Ammann, and V. Swarup, "A Weakest-Adversary Security Metric for Network Configuration Security Analysis," Proc. Second ACM Workshop Quality of Protection, pp. 31-38, 2006.
6. S. Jha, O. Sheyner, and J. Wing, "Two Formal Analyses of Attack Graphs," Proc. 15th IEEE Computer Security Foundations Workshop, June 2002.
7. New Non Path Metrics for Evaluating Network Security Based on Vulnerability