INTERNATIONAL JOURNAL OF ADVANCE RESEARCH, IDEAS AND INNOVATIONS IN TECHNOLOGY

ISSN: 2454-132X
Impact factor: 4.295
(Volume3, Issue5)

A Review On Security to Network using Security Metrics and Multisink Timestamp

Ms. Priyanka Patil Nagnath
P.G Student M.E Computer Science & Engineering,
Shriram Institute of Eng. & Technology,
Paniv, Maharashtra, India
priyankapatiln49@gmail.com

Prof. Dhainje Prakash B.
Head of CSE Dept.
Shriram Institute of Eng. & Technology,
Paniv, Maharashtra, India.
dhainjeprakash@gmail.com

Abstract: ***The emergence of wireless sensor networks (WSNs) can be considered one of the most important revolutions in the field of information and communications technology (ICT). Recently, there has been a dramatic increase in the use of WSN applications such as surveillance systems, battleground applications, object tracking, habitat monitoring, forest fire detection and patient monitoring. Due to limitations of sensor nodes in terms of energy, storage and computational ability, many security issues have arisen in such applications. As a result, many solutions and approaches have been proposed for different attacks and vulnerabilities to achieve security requirements. This paper surveys different security approaches for WSNs, examining various types of attacks and corresponding techniques for tackling these. We use multisink timestamp and attack graph based metrics. Multsink Timestamp technique finding out the attacking or sensing the attacking points among all networks in small period of time. For e.g. the large geographical areas where the volcanos or earthquakes may be occurred in future and these techniques finding out those areas provides the security to that area so that we can avoid the volcanos or earthquakes. For finding out the attacks in network we use three methods Normalized Mean of Path Lengths Metric, Standard Deviation of Path Lengths Metric, and Mean of Path Lengths Metric. These three metrics creates clusters of all networks and finding out only the attacking networks.***

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

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 Multisink, Measurements, Clustering, Metrics.

I. INTRODUCTION

Wireless sensor network is an area in wireless computing research which has been receiving a lot of attention recently. This can be mainly attributed to the huge number of potential applications of a wireless sensor network. As wireless sensor networks are primarily employed for sensing tasks, the architecture of the node in the network is fairly simple making them more energy efficient. This is where the main shortcoming of a wireless sensor network is. Due to the simple architecture it is difficult to ensure security in a wireless sensor network, as security protocols need to be lightweight enough to meet the energy constraints of the nodes. This paper comes up with a proposal to enhance an already existing protocol to improve both the security and efficiency of the wireless sensor network.

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. LITERAURE REVIEW

Wireless sensor networks (WSNs) can be used to monitor the interested region using multihop communication. Coverage is a primary metric to evaluate the capacity of monitoring. Connectivity also needs to be guaranteed so that the sink node receives all sensed data for future processing. In this paper, we study the m-coverage and n -connectivity problem under border effects. We consider the scenario where the heterogeneous sensor nodes are randomly distributed in a circular region. We first exactly derive the network m-coverage ratio that is provided by N sensor nodes by the mathematical formulas.

Paper Details:
Typically, any sensor can be turned on, turned off, or promoted cluster head, and a different power consumption level is associated with each of these states. We seek an energy-optimal topology that maximizes network lifetime while ensuring simultaneously full area coverage and sensor connectivity to cluster heads.
Methodology:
Minimizing energy dissipation and maximizing network lifetime are important issues in the design of applications and protocols for sensor networks. Energy-efficient sensor state planning consists in finding an optimal assignment of states to sensors in order to maximize network lifetime. For example, in area surveillance applications, only an optimal subset of sensors that fully covers the monitored area can be switched on while the other sensors are turned off. In this paper, we address the optimal planning of sensors' states in cluster-based sensor networks. Typically, any sensor can be turned on, turned off, or promoted cluster head, and a different power consumption level is associated with each of these states. We seek an energy-optimal topology that maximizes network lifetime while ensuring simultaneously full area coverage and sensor connectivity to cluster heads, which are constrained to form a spanning tree used as a routing topology. First, we formulate this problem as an Integer Linear Programming model that we prove NP-Complete. Then, we implement a Tabu search heuristic to tackle the exponentially increasing computation time of the exact resolution. Experimental results show that the proposed heuristic provides near-optimal network lifetime values within low computation times, which is, in practice, suitable for large-sized sensor networks.
Paper Details:
Dynamically adjust sensing coverage with guaranteed network connectivity, and is resilient to time asynchrony.
Methodology:
Sensor scheduling plays a critical role for energy efficiency of wireless sensor networks. Traditional methods for sensor scheduling use eith sensing coverage or network connectivity, but rarely both. In this paper, we deal with a challenging task: without accurate location informatio how do we schedule sensor nodes to save energy and meet both constraints of sensing coverage and network connectivity? Our approa utilizes an integrated method that provides statistical sensing coverage and guaranteed network connectivity. We use random scheduling f sensing coverage and then turn on extra sensor nodes, if necessary, for network connectivity. Our method is totally distributed, is able dynamically adjust sensing coverage with guaranteed network connectivity, and is resilient to time asynchrony. We present analytical resu to disclose the relationship among node density, scheduling parameters, coverage quality, detection probability, and detection delay. Analytic and simulation results demonstrate the effectiveness of our joint scheduling method

1) ***Published in:*** *24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings*

Paper Details:
To cover a set of targets with known locations when ground access in the remote area is prohibited, one solution is to deploy the sensors remotely, from an aircraft. The lack of precise sensor placement is compensated by a large sensor population deployed in the drop zone that would improve the probability of target coverage.
The Target algorithm
A critical aspect of applications with wireless sensor networks is network lifetime. Power-constrained wireless sensor networks are usable as long as they can communicate sensed data to a processing node. Sensing and communications consume energy, therefore judicious power management and sensor scheduling can effectively extend network lifetime. To cover a set of targets with known locations when ground access in the remote area is prohibited, one solution is to deploy the sensors remotely, from an aircraft. The lack of precise sensor placement is compensated by a large sensor population deployed in the drop zone that would improve the probability of target coverage. The data collected from the sensors is sent to a central node (e.g. cluster head) for processing. In this paper we propose un efficient method to extend the sensor network life time by organizing the sensors into a maximal number of set covers that are activated successively. Only the sensors from the current active set are responsible for monitoring all targets and for transmitting the collected data, while all other nodes are in a low-energy sleep mode. By allowing sensors to participate in multiple sets, our problem formulation increases the network lifetime compared with related work [M. Cardei et al] that has the additional requirements of sensor sets being disjoint and operating equal time intervals. In this paper we model the solution as the maximum set covers problem and design two heuristics that efficiently compute the sets, using linear programming and a greedy approach. Simulation results are presented to verify our approaches,

III. RELATED WORK

Investigations within the fields of threshold group-oriented aggregated Key schemes, threshold group aggregated Key schemes, Multisink Time Stamp schemes, and Threshold-Multisink Time Stamp schemes resulted in explicitly defining the properties of Threshold-Multisink Time Stamp schemes. Multisink Timestamp algorithm is to find out the Attacking network in the short period of time.We Provide the security to these all networks for preventing those networks from attack. So we can Transfer data or resources efficiently.
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

Shortest Path Metric captures the shortest distance to find out the attack in the Network.This metrics find out failure based nodes on network more fastly than other nework because of this metric chooses a shortest distance.
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.
The Shortest Path metric represents the length of the smallest attack path. The smallest attack path has the shortest distance from an attacker's initial state to the attackers desired goal state (i.e., where the security violation occurs).
The length function that determines the distance is dependent on the security engineer performing the attack graph analysis. The length of an attack path may be the number of conditions, the number of exploits, or the number of conditions and exploits that start from the attacker's initial state and proceeds in series to the attacker's goal state.

B. Number of Paths (NP) Metric

Number of path metric defines the one or more paths to reaches at the failure based nodes or attacking node.So that requires the more time for reaching at the attacking node. 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)
The Mean of Path Lengths metric captures changes that occur in the network that either increase or decrease security levels. Because this mean value is computed over the entire attack graph, any degradation that results in shorter path lengths will effect the mean path length if no other path increases in length to offset the degradation.
The Number of Paths metric is a value that represents the number of ways an attacker can leverage existing dependencies among vulnerabilities to violate a network's security policy. The Number of Paths metric is one that is designed to express how exposed a network is to path that is not the shortest path. Alternatively, an attacker may take a path different from the shortest path because the attacker could assume that the security engineer is using a shortest path analysis. With this knowledge, the attacker would avoid the shortest path because the path is likely to receive attention in the form of network activity monitors. Another reason an attacker may take a path that is not the shortest path is because the attacker's skill set may be better suited for a path that requires more effort.

C. Mean Path Length Metric (MPL)

The Mode of Path Lengths metric gives the attack path length that occurs most frequently. This metric represents another meaning of typical. In this context, typical refers to most frequent. If the security engineer is unable to determine the likelihood of an attacker traversing any attack path.
The Mean of Path Lengths metric represents the typical path length by obtaining the arithmetic mean for all path lengths. It gives an expected effort an attacker may expend to violate a network security policy. This metric is relevant because an attacker may not have the same view of the known vulnerabilities as the security engineer.

IV. 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.
Fig. 2 is example of attack graph. There are three
hosts in this network numbered from one to three. The attack graph in Fig. 2 corresponds to a network with a security policy that states that a user on host 1 should not be able to obtain exec (i.e., execute) or su (i.e., superuser) privileges on host 3. PwAuth

represents the ability to authenticate via the PwAuth program. XdmLog represents the X window display manager (xdm) login attack. WuFTPd represents an attack on the FTP server software wuarchiveftpd. In Fig. 2, the attacker could start from two different initial states: PwAuth(1,2) or exec(1). From PwAauth(1,2), the attacker can then leverage the WuFTPd(1,2) vulnerability to obtain exec privileges on host 2 (i.e., exec(2)). Alternatively, from the initial state of exec(1), the attacker could use the XdmLog(1,2) vulnerability to reach exec(2). From exec(2), the attacker can use the WuFTPd(2,3) vulnerability to reach either goal state (i.e., su(3) or exec(3)).

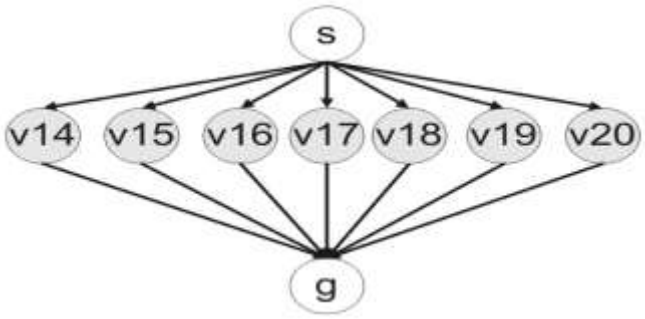

Fig1 Attack Graph with vulnerabilities 14 through 20.

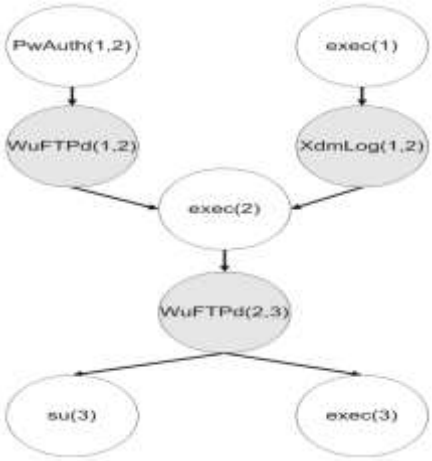

Fig2. An Example Attack Graph

A condition in an attack graph 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 AND FUTURE WORK

The main aim of this project is to introduce a secure Multisink Time Stamp scheme. To reach this objective, the secure and optimally efficient Straw-man type aggregated Key variant, GES, was extended to a multiparty setting to yield a Multisink Time Stamp scheme, which provides a guaranteed traceability property. The proposed Multisink Time Stamp scheme was shown to satisfy all of the specified security requirements and fulfills the stronger break-resistant property. The Multisink Time Stamp aggregated Key scheme thus remains secure, even if the threshold cryptosystem has been broken, i.e.the group secret or individual secret shares are known or controlled by an adversary.That means from large network system find out the all small networks during particular time period which has been defect .And provide the security to all the network for prevention of attack.

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.

RESULT ANALYSIS

In this section, we show the results of using compare Graphs for two sets of randomly generated attack graphs. The number of paths in the attack graphs are uniformly distributed between 1 and 2,000 attack paths. The path lengths is uniformly distributed between 1 and 50. 1,000 randomly generated attack graphs are assigned to set and another 1,000 randomly generated attack graphs are path analysis attack graph-based security metrics. We have detailed how to use the above mentioned metrics with our proposed suite of metrics to measure the security of networks under consideration. We have shown through simulated results that in many instances, our approach for metric combination is able to decide which of two attack graphs correspond to a more secure network.

ACKNOWLEDGEMENT

The proposed system is based on IEEE Transaction paper under the title An Authentication Protocol for Clustered Wireless Sensor Networks published in IEEE TRANSACTIONS in computer science volume 8,no 3,March / April 2017

REFERENCES

[1] Joel Joy Manjaly and J Sandeep An Authentication Protocol for Clustered Wireless Sensor Networks International Journal of Advanced Research in Computer Science Volume 8, No. 3, March – April 2017

[2] Nwokedi Idika,Bharat Bhargava, Fellow, " Extending Attack Graph-Based Security Metrics and Aggregating Their Application",published in IEEE transactions on dependable secure computing,vol.9,no.1,january/february 2012.

[3]V.Thiruppathy Kesavan, S. Radhakrishnan "Multiple Secret Keys based Security for Wireless Sensor Networks International Journal of Communication Networks and Information Security (IJCNIS) Vol. 4, No. 1, April 2012.

[4]. 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.

[5]. 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.

[6]. 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.

[7]. S. Jha, O. Sheyner, and J. Wing, "Two Formal Analyses of Attack Graphs," Proc. 15th IEEE Computer Security Foundations Workshop, June 2002.

[8] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An Attack Graph-Based Probabilistic Security Metric," Proc. Data and Applications Security (DAS '08), pp. 283-296, 2008.

[9] Patil P.N, Dhainje P.B,Deshmukh P.K "Attack Graph Based Security Merics And Other Metrics For Producing Security To Computer IJCSIT vol 6(2)2015 "

