Anshula et al. International Journal of Institutional & Industrial Research ISSN: 2456-1274, Vol. 1, Issue 3, September-December 2016, pp.1-5

A Dynamic Methodology to Experimenting Security of Networks Using Attack

Anshula[1], Krishan Kumar[2]

[1]Assistant Professor, Computer Science Department, Kalindi College
[2]Assistant Professor, Department of Computer Science, Kalindi College, University of Delhi

Abstract: **The past ways to deal with measuring system security are most in light of the speculation that the related source information can be known well and genuinely. Be that as it may, by and by, it is extremely hard to get all the related precise source information . In this paper, we propose an adaptable approach in view of assault charts to measuring security of critical assets in powerless system, which could draw out the precise consequence of measuring system security with fragmented info information. Another key change is showing the retrogressive iterative calculation to take care of the issue of cyclic assault ways in measuring security utilizing assault charts. In the meantime, the recreation test shows the calculation can be connected to the vast assault charts.**

Keywords: Network Security

1. 1. Introduction

Since it is by all accounts exceptionally hard to ensure no vulnerabilities in the objective system, it is essential for security oversee to gauge security of vital assets in the helpless system. In the examination of the vulnerabilities, certain vulnerabilities may appear to be adequate dangers when considered in segregation. Be that as it may, a gatecrasher can frequently penetrate an apparently very much monitored organize through a multi-step interruption, in which every progression gets ready for the following. The majority of past measure approaches overlook the potential hazard. Assault charts give the missing data about connections among the known vulnerabilities, in this manner permit us to consider potential assaults and their results. Lingyu Wang proposed a structure of measuring system security utilizing assault charts in , in spite of the fact that it couldn't work in the functional assault diagrams with cyclic assault ways.

There is likewise a basic yet overlooked issue in the past investigation of measuring system security. To quantify arrange security, the related source information must be referred to, for example, the endeavor achievement likelihood, which is characterized in segment 4.1. In any case, practically speaking, security oversees will discover it is extremely hard to acquire all the related exact source information

Some of them couldn't be gotten for some situation, for example, abuse achievement probabilities of new adventures for the most recent found vulnerabilities. Under this case, the past way to deal with measuring system security couldn't work, since they depend on the speculation that the related source information might be known well and genuinely. In the investigation of the system security against interruption, any positive counsel is valuable to security controls. The test confronted by the security oversee is in this way: How to quantify security of pivotal assets in the powerless system, with fragmented info information.

In this paper, we propose an adaptable approach in light of assault diagrams to measuring security of critical assets in helpless system. Its first key change is that it utilizes the regressive iterative calculation to take care of the issue of cyclic assault ways in assault charts and shows the calculation can be connected to the substantial assault diagrams through recreation explore. The second change is that the new measure approach can be completed with deficient information and even for some situation it might accomplish the exact consequence of measuring system security (an illustration will be given in segment 5). The noteworthiness is acquainted with assess the truant information's effect on the last outcome esteem. In a word, the measure approach has the trademark that progressively the information source information, more precise the aftereffect of measure.

Whatever is left of this paper is composed as takes after. The following area surveys related work. Segment 3 talks about formally assault diagrams. Segment 4 expresses the way to deal with measuring system security. Segment 5 gives a case to outline the proposed technique. At last, Section 6 finishes up the paper.

2. 2. Related Work

A diagram of different issues significant to security measurements is given in [1]. The NIST's endeavors on institutionalizing security measurements are reflected in the Technology Assessment: Methods for Measuring the Level of Computer Security [2] and all the more as of late in the Security Metrics Guide for Information Technology Systems [3]. The last depict the present

condition of utine of security measurements, for example, that required by the Federal Information Security Management Act (FISMA). In light of an exponential appropriation for an assailant's prosperity rate after some time, the methodologies utilize a Markov show and the MTTF (Mean Time to Failure) to gauge security given in [4,5]. Another arrangement of work measures how likely a product is powerless against assaults utilizing a measurements called assault surface [6]. These works permit a halfway request to be built up on various system arrangements in light of their relative security. Another approach measures the relative danger of various setups utilizing the weakest assailant display, which is the minimum conditions empowering an assault in [7]. These methodologies are altogether in light of the theory that the related source information can be known well and genuinely. Since the speculation is not generally genuine, our approach centers the measure security with fragmented related source information.

The assault diagram demonstrates all the assault ways to the objective. There are two representations of the assault chart. One is the state-based assault chart in which hubs are all worldwide state. It demonstrates all the assault ways unequivocally. The development and examination in view of the express assault diagram incorporates [8-14]. The express assault diagram confronts a genuine versatility issue, in light of the fact that the quantity of such arrangements is exponential in the quantity of vulnerabilities duplicated by the quantity of hosts. To evade such combinatorial blast, another reduced representation of assault charts in which hubs are endeavors or conditions is proposed in [15-18]. The monotonicity supposition underlies this speak to ation, i.e., an aggressor never gives up any got ability. This more up to date representation can therefore keep precisely one vertex for every adventure or security condition, prompting to an assault diagram of polynomial size (in the aggregate number of vulnerabilities and security conditions). In this paper we should expect such a reduced representation of assault diagrams.

Nearest to our work, Lingyu Wang proposed a structure of measuring system security utilizing assault diagrams, in spite of the fact that it couldn't work in the down to earth assault charts with cyclic assault ways and is likewise based the above irrational theory in.

3. Attack Graphs Semantic

Our approach is based on the compact representation of attack graphs, and we formally define it.

Definition 1 Let *AP* be a set of atomic propositions,an attack graph is a tuple $AG = (C_0, T, C_d, E, L, C_g)$,
where C_0 is a set of initial condition nodes, T is a set of exploit nodes, C_d is a set of intermediate condition nodes, $C_g \subseteq C_d$ is a set of the intruder's goal condition nodes, $L : C_0 \cup C_d \cup C_g \rightarrow AP$ is a mapping function from a node to its corresponding atomic proposition,

To encourage understanding the assault diagram, it is advantageous to translate an assault chart as a straightforward rationale program as takes after. Every condition in the assault diagram is deciphered as a rationale variable. The interdependency amongst adventures and conditions now gets to be rationale suggestions including the two connectives AND as well as, with AND between the conditions required by every endeavor or potentially between the endeavors inferring every condition.

Property 1 For every exploit node τ, let $\mathrm{Pre}(\tau)$ be the set of τ 's pre-conditions and $\mathrm{Post}(\tau)$ be the set of τ 's post-conditions, then $(\wedge L(c_i)) \rightarrow L(c'_k)$, where $c_i \in \mathrm{Pre}(\tau)$, and $c'_k \in \mathrm{Post}(\tau)$, that shows when all the pre-conditions of exploit τ are true, every post-condition of exploit τ is true.

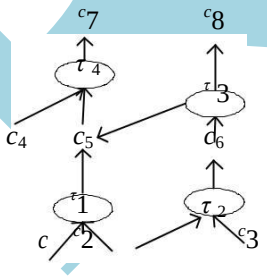

Figure 1 the First Example of Attack Graphs

Definition 2 Let $\tau_1 \tau_2 ... \tau_l$ is a finite sequence of exploits in attack graph, where $\tau_i \in T$ for all $0 \le i \le l$, if $\forall c \in \mathrm{Pre}(\tau_i)$, $c \in \cup_{k=1}^{i-1} \mathrm{Post}(\tau_k) \cup C_0$, which shows thefront exploit prepares conditions for the latter exploit, then we define an *attack path* as the finite sequence of exploits such that $\exists c' \in \mathrm{Post}(\tau_l)$, $c' \in C_g$, which shows one of the last exploit's post-conditions is the goal condition.

Figure 1 shows a simple example of attack graphs, where $C_0 = \{c_1, c_2, c_3, c_4\}$, $T = \{\tau_1, \tau_2, \tau_3, \tau_4\}$, $C_d = \{c_5, c_6\}$, $C_g = \{c_7, c_8\}$ .The intruder can achieve the goal condition c_7 through the attack path $\tau_1\tau_4$ or $\tau_2\tau_3\tau_4$, and the goal condition c_8 through the attack path $\tau_2\tau_3$

4. Approach to Measure Security

In this area, we first talk about different probabilities in the assault chart based measure of the system security. Next, on the suspicion that all the info probabilities information could be procured, we exhibit the regressive iterative calculation to gauge security for assault charts with cycles. At last, deserting the above supposition, we proposed an approach to measuring network security with incomplete input probabilities data.

4.1. Probabilities in Attack Graphs

At the point when each pre-state of one adventure are acquired, we characterize it as the performable endeavor . The fruitful event of performable endeavor lies in execution trouble, for example, the prerequisite for the interloper's assault capacity and abilities. We utilize abuse achievement likelihood Eprob(τ) to denote performance difficulty the Performable exploitτ , whose esteem might be assessed by security specialists, and utilize fruitful event likelihood O prob(τ) to signify the effective event probability of the adventure τ by interloper.

We utilize condition got likelihood Cprob(c) to indicate the probability of the condition c acquired by interloper. When one performable endeavor happens effectively, its each post-condition will be valid. For the situation that more than one adventures achieve the condition c , we consider the interloper will picks the endeavor with the best event likelihood. Along these lines, the condition got likelihood of condition c can be known through the accompanying recipe:

$\text{Cprob}(c) = \text{Max}(\text{Oprob}(\tau_i))$, where $\tau_i \in \text{post}(c)$.

Initially we assign $\text{Cprob}(c_i) = 1$, where $c_i \in C_o$. The *successful occurrence probability* of exploitτcan becomputed through the formula below:

$$\text{O prob}(\tau) = \text{Eprob}(\tau) \cdot \text{Cprob}(c_1) \cdots \text{Cprob}(c_n),$$

where $c_i \in \text{Pre}(\tau)$.

Definition 3 Given an attack graph $AG = (C_0, T, C_d, E, L, C_g)$, we define the *security risk* as $\text{Max}(\text{Cprob}(c_i))$ such that $c_i \in C_g$.

In the attack graph of figure 1, We suppose that $\text{Eprob}(\tau_1) = 0.9$, $\text{Eprob}(\tau_2) = 0.05$, $\text{Eprob}(\tau_3) = 0.6$, $\text{Eprob}(\tau_4)$, then .

4.2. Backward Iterative Algorithm

The most of practical attack graphs have cycles in attack paths, such as the second example of attack graphs in figure 2, where the attack path $\tau_1\tau_3\tau_4\tau_3\tau_5$ has cycles. In the practical network intrusion, the intruder generally could not choose the cyclic attack path, but removing any exploit in the attack graph will lose useful acyclic attack paths[15]. As a consequence, the challenge is that the above iterative approach to computing *security risk* will be disabled, and the same problem exists in [19]. In the remaining of this section, we propose the *backwarditerative algorithm* to solve the problem.

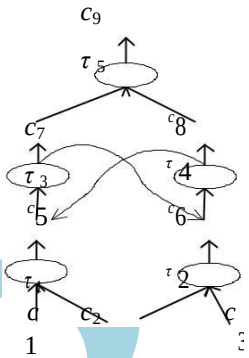

Figure 2 the Second Example of Attack Graphs

To facilitate computing *security risk*, we introduce the placeholder condition *g* and the placeholder exploit ε_i whose pre-condition is $c \in C_g$, and post-condition is *g* . In the attack graph, ε_i and *g* do not correspond to any real exploit and condition. The corresponding attack graph of the simple example in Figure 1 introduced ε_i and *g* shows in Figure 3. Obviously, when let $\text{Eprob}(\varepsilon_i) = 1$,the attack graph (C_0, T, C_d, E, L, C_g) has the same *security risk* as the attack graph $(C_0', T', C_d', E', L, g)$, where $T' = T \cup \{\varepsilon\}$, $C_d' = C_d \cup C_g$, $E' = E \cup \{(c_j, \varepsilon_i), (\varepsilon_i, g) \mid c_j \in C_g\}$. In the following discussions, we consider the attack graph as $AG = (C_0, T', C_d', E', L, g)$

The detail of the regressive iterative calculation is appeared in figure 4. In the event that the information hub N is the condition node(line 2-13), the arrival esteem is the condition acquired likelihood of condition N(line 14-25), in the meantime, if the information hub N is the endeavor hub, the arrival esteem is the effective event likelihood of adventure N. In the pragmatic system assaults, the gatecrasher for the most part does not utilize similar endeavors to acquire the assault capacity. In this manner, a set way is acquainted with record the profundity first in reverse traversal follow. On the off chance that the hub is as of now in the way, the likelihood of the node(condition or endeavor) is 0, which implies that the adventure does not show up twice in a similar assault way. Given the assault chart and every adventure's endeavor achievement likelihood, we could obtain the security

*risk*through the procedure prob_gen(*g*,path), where theset *path* is initially empty.

cyclic assault ways to the non-cyclic assault ways. As a result, it infers that the multifaceted nature of the calculation directly lies in the quantity of the potential non-cyclic assault ways. Instinctively we realize that the assault charts with more cyclic assault ways have the more non-cyclic assault ways. To determinate the regressive iterative calculations is adaptable and can be connected to huge assault charts, we run the calculation to figure the security danger of various substantial assault diagrams created arbitrarily with various the quantity of beginning conditions(No.IC), distinctive the quantity of conditions(No.conditions), diverse the quantity of

misuses, diverse the quantity of edges(No.edges). The analysis is done in PC with CPU 1.6Ghz and Memory 512 MB and the estimations of endeavor achievement probabilities are additionally created haphazardly.

The result of experiment indicates that this method can be applied to large attack graphs. However, the CPU Time depends on the characteristic of attack graphs, such as the attack graphs of D and E.

Table 1 the Result of CPU Time

Attack Graph	No. IC	No. conditions	No. exploits	No. edges	CPU Time (sec)
A	34	75	49	121	0.4
B	46	95	67	169	0.6
C	81	236	86	1032	1.1
D	202	322	99	1514	2..3
E	195	295	104	5207	10.4

4.3. Measuring with Incomplete Input Data

To compute security risk, exploit success probability of each exploit involved in attack graph is necessary to be known. But in practice, it is very difficult to obtain all the accurate probabilities. Some of them may not be obtained in some case, e.g. the exploit success probabilities of new exploits for the latest discovered vulnerabilities. We believe that any advice is useful in defending the network security against intrusion. Thus, the other challenge in the face of the measuring security is how to computing security risk with the incomplete source data.

There is an interesting phenomenon that *exploitsuccess probabilities* of some exploits varying in a givenrange does not change the final value of *security risk*. In other words, some inaccurate exploit success probabilities have no effect on the final value of security risk. Even in the extreme case, the probabilities assigned to the any value in the domain do not affect the final value of security risk .For example, in the first example of attack graph in figure 1, when prob(τ_3) is assigned to 1 or 0, the

security risk is still 0.72. It means that we could obtain the same accurate result without the value of Eprob(τ_3) .

Based on the above fact, we propose an approach to computing security risk with incomplete source data, and introduce the *creditability* to evaluate the absent data's impact on the final result.

We partition the adventures into two classifications regarding whether their endeavor achievement probabilities could be acquired. One is the adventures with the endeavor achievement probabilities evaluated by various security specialists and

signified as the set Ta . The other classification is the new found adventures with the obscure probabilities and indicated as the set Tl .

On the assumption that Eprob(τ) =1 where $\tau \in T_l$, we could obtain the *maximal security risk* (denoted as *MaxSecRisk*) through the procedure prob_gen(g , path) in the worst case. At the same time, on the assumption that Eprob(τ) =0, where $\tau \in T_l$, we could also obtain the *minimal security risk* (denoted as*MinSecRisk*) in the bestoptimistic case. From the conservative defender's perspective, we define the final security risk as *maximalsecurity risk*. In the process of measure, we find that someexploits' Eprob values do not affect the final outcome, such as the Eprob(τ_3) mentioned in the above, but some exploits' Eprob values determines the final outcome

sensitively. We introduce the *creditability*θ to quantitatively evaluate the absent data's impact on the final result and its value is computed through the formula below:

$$\theta = \frac{MinSecRisk}{MaxSecRisk} \times 100\%$$

When the value of *creditability* equals to 1, it means that the absent data has no impact on the final value of security risk. In other words, despite some source data has not been acquired, the measure result is still accurate. When the value of *creditability* equals to 0, it means that the final measure result is invalid and not helpful to security administer for some crucial source data being absent. In the process of measuring, we should do our endeavor to avoid such situations

5. Example

To delineate the normal for our approach all the more obviously, we apply it to an outstanding case in the investigation of assault diagrams. In the accompanying

application case, the aggressor's machine is signified machine 0, and the two casualty machines are meant 1 and 2, individually. The points of interest of the assault situation, (for example, organize topology, accessible administrations, working frameworks, and so on.) are not required here, in spite of the fact that the intrigued peruser can allude to [8] and [9] for such subtle elements.

Figure 6 shows the attack graph of this example. In this figure, exploits appear as ovals, and conditions appear as plain text (except the goal condition, which is marked with a triple octagon). Numbers in parenthesis identify associated machines. For example, root(2) denotes root privilege on machine 2, and rsh(2,1) denotes the execution of the *rsh* exploit from machine 2 to machine 1.

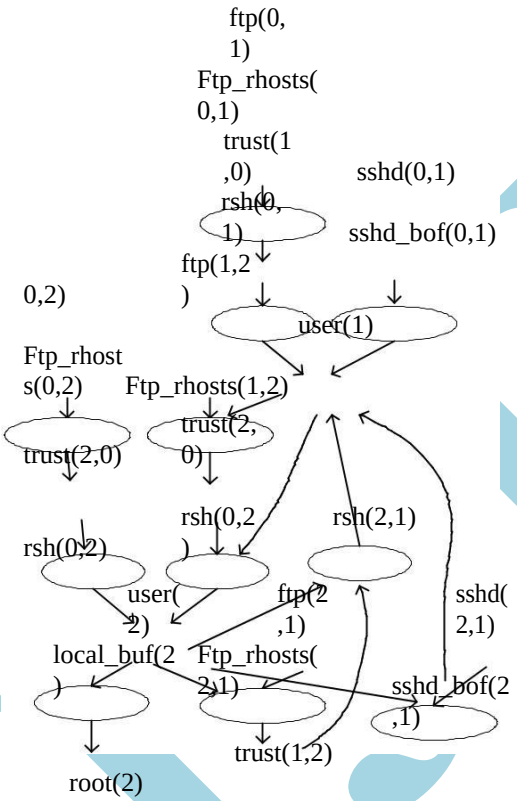

Figure 6 the Attack Graph of the Well-known Example

The table 2 shows three groups of the hypothetical values of exploit success probabilities and the corresponding values of security risk and creditability computed through our approach. The symbol "-" indicates the corresponding value is absent. The first result is invalid and does not benefit the security administer for the source data is so scarce that the value of creditability is equal to 0. Fortunately, after obtaining the exploit success probability of rsh(2,1), we know the security risk is 0.162, and the creditability is 100%, which means that the result is accurate, although the source data is still scarce. Furthermore, when the exploit success probability of rsh(0,2) is changed to 0.1, the security risk is 0.54, but creditability is 30%, which means the accuracy degree of result is very low and some absent data needs to be known for higher accurate measure result.

Table 2 the Input Data and Measure Result

ftp_rhosts (0,2)	ftp_rhosts (0,1)	sshd_bof(0,1)	rsh(0,2)	rsh(0,1)
-	-	0.6	0.2	0.6
-	-	0.6	0.2	0.5
-	-	0.6	0.6	0.6
rsh(1,2)	ftp_rhosts (1,2)	ftp_rhosts (2,1)	sshd_bof(2,1)	local_b of(2)
0.6	0.5	--	-	-
0.6	0.5	-	-	0.8
0.6	0.5	-	-	0.9
rsh(2,1)	security rsik	creditabili ty		
-	0.18	0		
-	0.192	96%		
-	0.32	30%		

6. Conclusion

In this paper, we propose an adaptable approach in light of assault charts to gauge security of pivotal assets in

powerless system. The primary key change is displaying the retrogressive iterative calculation to take care of the issue of cyclic assault ways in assault charts and demonstrate the calculation can be connected to the substantial assault diagrams through reproduction try. The second change is that the measure approach can be done with inadequate info information. Later on research, we have to decide the essential endeavors without whose adventure achievement probabilities, the measure result is dependably 0. The answer for the issue will be helpful to stay away from the invalid measure result

References

[1] Applied Computer Security Associates. Workshop on. *InInformation Security System Scoring and Ranking*, 2001.

[2] National Institute of Standards and Technology. Technology assessment: Methods for measuring the level of computer security. *NIST Special Publication* 500-133, 1985.

[3] M. Swanson, N. Bartol, J. Sabato, J. Hash, and L. Graffo.Security metrics guide for information technology systems. *NIST Special Publication* 800-55, 2003.

[4] R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Trans. Software Eng*., 25(5):633–650, 1999.

[5] M. Dacier, Y. Deswarte, and M. Kaaniche. Quantitative assessment of operational security: Models and tools.
Technical Report 96493, 1996.

[6] J. Wing P. Manadhata. An attack surface metric. *In FirstWorkshop on Security Metrics* (MetriCon), 2006.

[7] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup. A weakest-adversary security metric for network configuration security analysis. *In Proceedings of the 2ndACM workshop on Quality of protection*, pages 31–38, NewYork, NY, USA, 2006. ACM Press.

[8] S. Jha, O. Sheyner, and J.M. Wing. Two formal analysis of attack graph. *In Proceedings of the 15th Computer SecurityFoundation Workshop* (CSFW'02), 2002.

[9] O. Sheyner, J. Haines, S. Jha, R. Lippmann, and J.M.Wing. Automated generation and analysis of attack graphs. *InProceedings of the 2002 IEEE Symposium on Security and Privacy* (S&P'02), pages 273–284, 2002.

[10] D. Zerkle and K. Levitt. Netkuang - a multi-host configuration vulnerability checker. *In Proceedings of the6th USENIX Unix Security Symposium* (USENIX'96),1996.

[11] C. Phillips and L. Swiler. A graph-based system for network-vulnerability analysis.*In Proceedings of the NewSecurity Paradigms Workshop* (NSPW'98), 1998.

[12] R. Ritchey and P. Ammann. Using model checking to analyze network vulnerabilities. *In Proceedings of the 2000*

IEEE Symposium on Research on Security and Privacy

(S&P'00), pages 156–165, 2000.

[13] R. Ritchey, B. O'Berry, and S. Noel. Representing TCP/IP connectivity for topological analysis of network security. I*nProceedings of the 18th Annual Computer Security Applications Conference* (ACSAC'02), page 25, 2002.

[14] S. Jajodia, S. Noel, and B. O'Berry. Topological analysis of network attack vulnerability. In V. Kumar, J. Srivastava, and A. Lazarevic, editors, *Managing Cyber Threats: Issues,Approaches and Challenges*. Kluwer Academic Publisher,2003.

[15] Xinming Ou, Wayne F. Boyer, and Miles A. McQueen. "A Scalable Approach to Attack Graph Generation".

Proceedings of the 13th ACM conference on Computer and communications security,pp. 336 – 345, 2006.

[16] X. Ou, S. Govindavajhala, and A. Appel. MulVAL: A logicbased network security analyzer. *In Proceedings of the14th USENIX Security Symposium*, pages 113–128, 2005.

[17] P. Ammann, D. Wijesekera, and S. Kaushik. Scalable, graph-based network vulnerability analysis. *In Proceedingsof the 9th ACM Conference on Computer and Communica-tions Security* (CCS'02), pages 217–224, 2002.

[18] Lingyu Wang,Anoop Singhal,Sushil Jajodia, Toward measuring network security using attack graphs,*Conferenceon Computer and Communications Security Proceedings of*

the 2007 ACM workshop on Quality of protection, pages 49 – 54,2007

