ATLANTIS PRESS
Advances in Computer Science Research, volume 50
4th International Conference on Electrical & Electronics Engineering and Computer Science (ICEEECS 2016)

An approach to evaluate network security risk based on attack graph

Xiaoyun Hu[1,2,a], Yang Yu[1,2,b] and Chunhe Xia[1,2,c]

[1] Beijing Key Laboratory of Network Technology, China

[2] School of Computer Science and Engineering, Beihang University

[a] xiaoyun_hu@163.com, [b] kiko441500@163.com, [c] buaaxch@126.com

Keywords: risk evaluation, attack graph, vulnerability analysis

Abstract. Facing with plethora network security events, network security risk evaluation is an effective method to prevent and respond to these security problems. Ignoring possible changes maybe occurred, traditional network security risk evaluation only emphasizes the preventive management in advance. This article presents an approach to explore the probability of network attributes to be breached accurately in Bayesian Attack Graph. In particular, our approach extends BAG with observation node that can be used to imply and adjustment compromising probability timely and dynamically.

Introduction

In theory, the source of network security risk mainly is direct and indirect network attack exploitations. Therefore, we conduct on network security risk evaluation with the purpose of applying guidance to strong network security defense. Based on attacking process, we classify defense work into two stages: predictable defense before attack exploitation, responding defense after attack exploitation.

Network security risk evaluation, as an active defense means, can depict the network security situation. The way to reduce the negative effects after attack exploitation is determined by detection techniques and response techniques. Traditional artificial responding mechanism intensified time lagging, even reduced prosthetic affect.

To alleviate such drawbacks above, we propose to use Bayesian Graph Attack with observation nodes to acquire probability of network attributes and exploitation in this paper. Please note that the generation of Bayesian Attack Graph is out of discussion range in this article, so we just assume the BAG has been generated in our previous work.

Related Work

Attack graphs are used as a vital security risk evaluation model for analyzing the inter-dependencies of attack-springboards and security attributes[1,2]. Due to the similarity that Bayesian network and attack graph both provides causal relationship between random variables, researchers began to model network vulnerabilities and quantificat network security risk by Bayesian Network(BN)[3]. Homer et al. [4] presented a quantitative model to measure the likehood that an attack means can be completed . They brought the notion of d-seperation within a Bayesian network to settle the shared dependency problem among different attack paths. Frigault et al.[5] proposed a probability metrics model based on attack graphs. They allocate the conditional probabilities to every nodes in attack graph to caculate the probability of node with causal relationshaip, which represented the overall security risk in network. They assigned each service a security risk signature by analying the vulnerability severity and exploiting difficulty with Bayesian network.

However, traditional ways to construct attack graph are just based on network basic attributes, such as vulnerabilities, connections, services and protocol information, which can't adjust dynamically to adapt to the network security event occurrence[6,7]. In order to deal with the evolving nature of vulnerabilities, Frigault et al. [8]continue to reseach a Dynamic Bayesian Networks(DBN)

model,which is a sequence of BNs corresponding to a particular instant of time, to incorporate temporal factors. Poolsappasit formally proposed Bayesian Attack Graphs and use the model to correlate alerts, and hypothesizing missing and predict future attacks [9] .

Network security risk evaluation with BAG

Attack Graphs represent prior knowledge about vulnerabilities, network connections, services and privilege. Bayesian Network can be used to caculate quantitative probabilities combining all corresponding system security network conditions. We extends the definition of Bayesian Attack Graph (BAG), and the BAG is expressed by $\varepsilon_{BAG} = (N, E, O, R)$,where N is the set of attributes node, E presents the set of exploitation nodes, O is the observation events and R is the tuple (N_{pre}, E_{post}) or (E_{pre}, N_{post}).

The network security risk consists of Static Risk that obtained by conditional probability ditribution table (CPDT) of precondition variables in BAGs and Dynamic Risk that assessed with static network attributes and dynamic observation events. We use the uniform way to evaluate network security risk value , given as

$$R_{risk} = S_{pro} * C_{val} . \quad (1)$$

Where S_{pre} is the propability of breaching the target attribute node, and C_{val} is the asset value of the corresponding nodes. In this paper, we focus on quantificating the propability of breaching attribute.

Conditional probability distribution table (CPDT) of every node is assigned by system administrator with the knowledge of exploitation difficulty of vulnerability, the probability of breaching security successfully and the relationship of attribute's precondition nodes.

For vulnerabilities, The Common Vulnerability Scoring System (CVSS) of FIRST has developed a mature method to standardize the metrics of individual vulnerability, involving base metrics, temporal metrics and environment metrics. We adopt the exploitability sub-score in CVSS to depict the exploitation difficulty of vulnerability, which is composed of the access vertor(Av), access complexity(Ac), access complexity (Au), and all related metrics can be found in Common Vulnerabilities and Exposures(CVE) and CVSS guide. Due to exploitability sub-score is a decimal number from 0 to 10, so we normalize it to imply the probability $P(e_i)$ of implementing the attack exploitation as the following , where $e_i \in (N_{pre}, E_{post})$.

$$P(e_i) = 2 * Av * Ac * Au \quad (2)$$

For $s_i \in (E_{pre}, N_{post})$, we use the propability of the exploitation to breach security successfully. Normally, the vulnerability exploitation's success rate is set as 1, others should be assigned by system administrator and expert system.

The arcs in BAGs means the causal relationship of attributes node N_i and its parents node $Pa(N_i)$ and the relationship r_i implies the decompositon dependency of them. For And-dependency , the attributes node N_i may be compromised only when all of its' parent nodes $Pa(N_i)$ has been compromised successfully, and every N_i is Bernoulli random priors and every exploitation e_i for $N_j \in Pa(N_i)$ is independent event. While for Or-dependency, the attributes node N_i can be compromised just one of its' parent nodes $Pa(N_i)$ has been compromised, and the attributes node is similar to noisy-OR nodes[3]. Every instance consisting in CPDT is related with $P(e_j)$, for $N_j \in Pa(N_i)$, and r_i as follows.

(1). If r_i is And,

$$P(N_j \mid Pa[N_j]) = \begin{cases} 0, \exists N_i \in Pa[N_j], N_i = 0 \\ \prod_{N_i \in Pa[N_j]} P(e_i), otherwise \end{cases} \quad (3)$$

(2). If r_i is Or,

$$P(N_j \mid Pa[N_j]) = \begin{cases} 0, \forall N_i \in Pa[N_j], N_i = 0 \\ 1 - \prod_{N_i \in Pa[N_j]} [1 - P(e_i)], otherwise \end{cases} \quad (4)$$

By assigning CPDT to every nodes in the BAG, the joint probability of discrete Bernoulli variable set $N = \{N_1, N_2, ..., N_n\}$ can be inferred by the product of every node's conditional probability that depends on $Pa(N_i)$, also known as Bayesian chain rules:

$$P(N_1, N_2, ..., N_n) = \prod_{i=1}^{n} P(N_i \mid pa(N_i)). \quad (5)$$

Consider the simple BAG in Fig 1 shows, node A,B,C represent network security attribute of initial attack state. The probability of these nodes should be assigned by experienced system administrator and system historical data and each decimal in arcs $P(e_j)$ indificates the exploitation difficulty caculated by CVSS metrics.

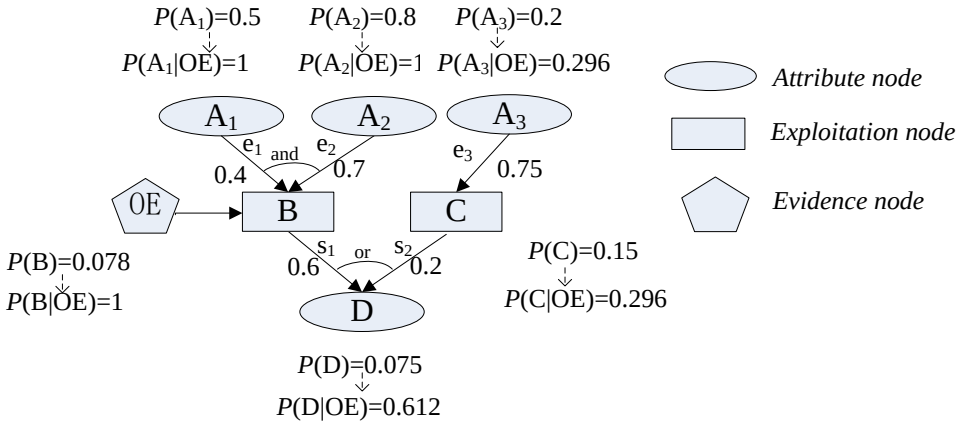

Fig 1 A simply example of Bayesian Attack Graph with decompositon

The CPDT for node B and node D in Fig 1 can be obtained as Table 1 and Table 2 :

Table 1 CPDT for node B in Fig 1

A_1	A_2	B	
		P(B=0)	P(B=1)
0	0	1	0
1	0	1	0
0	1	1	0
1	1	$1 - p(e_1 \cap e_2)$ =0.72	$p(e_1 \cap e_2) = p(e_1) * p(e_2)$ =0.28

Table 2 CPDT for node D in Fig 1

B	C	D	
		P(D=0)	P(D=1)
0	0	1	0
1	0	$1 - p(s_1)$ =0.4	$p(s_1)$ =0.6
0	1	$1 - p(s_2)$ =0.8	$p(s_2)$ =0.2
1	1	$p(\neg s_1 \cap \neg s_2)$ =0.32	$1 - p(\neg s_1 \cap \neg s_2)$ =0.68

The unconditional probability of node B can be caculated by CPDT and initial probability as follows.

$$P(B) = \sum_{A_1, A_2 \in \{0,1\}} P(B \mid A_1, A_2) * P(A_1) * (A_2) \approx 0.078 \quad (6)$$

$$P(D) = \sum_{A_1, A_2, A_3, B, C \in \{0,1\}} P(D \mid A_1, A_2, A_3, B, C) \approx 0.075 \quad (7)$$

Alarms produced by Firewall, IDS and Anti-virus software in network running will influence the probability of attribution node and exploitation node, and then the whole security risk of network, which will be defined as Observation Node in our BAGs. The observation node is not deterministic owing to the accuracy rate of the components which alerts it, so $P(Inf \mid OE) \leq 1$. In the case of Fig 1, we hypothesize the accuracy rate of observation node OE is 1 and it implies the exploitation of node B did happen, so $P(B \mid OE) = 1$. Then we can caculate $P(N_i \mid OE)$ for other nodes by posterior probability as Eq.8， where Inf means the nodes is influnced by observation node directly . We use the posterior probability to guide the other nodes in the process of dynamic adjustment.

$$P(Ni \mid OE) = \frac{P(Inf \mid Ni) * P(Ni)}{P(Inf)} * P(Inf \mid OE) \tag{8}$$

By adding the observation node, we can find the posterior probability of every node is higher than ever before in Fig 1. The unconditional probability is aiming to organize a defense previously, and the posterior probability is used to defense the network security with critical place that has been breached.

Conclusion

We developed an approach to assess network security risk by calculating the probability of each nodes, including attribution nodes and exploitation nodes, to be compromised in BAG dynamically. Our approach takes CVSS metrics as vulnerability exploitation difficulty and hit rate as input , use CPDT and Bayesian theory to explore the risk quantization value for preparatory work and emergency work. However, the Bayesian Attack Graph is limited to explore large scale network, we will conduct relevant to researches on how to apply it to more hosts and services.

Acknowledgements

The project is supported by the National Natural Science Foundation of China (Grant No.61170295) and the Joint Funds of the National Natural Science Foundation of China.

References

[1] D. Saha, Extending logical attack graphs for efficient vulnerability analysis., ACM Conference on Computer and Communications Security, CCS 2008, Alexandria, Virginia, Usa, October (2008).
[2] S. Noel, E. Robertson, and S. Jajodia, Correlating intrusion events and building attack scenarios through attack graph distances. (2004)
[3] Y. Liu, and H. Man, Network vulnerability assessment using Bayesian networks. Proceedings of SPIE - The International Society for Optical Engineering (2005).
[4] J. Homer, X. Ou, and D. Schmidt, A sound and practical approach to quantifying security risk in enterprise networks. (2010).
[5] M. Frigault, and L. Wang, Measuring Network Security Using Bayesian Network-Based Attack Graphs, Computer Software & Applications, Compsac 08 IEEE International, (2008), p. 698-703.
[6] M.S. Barik, and C. Mazumdar, A Graph Data Model for Attack Graph Generation and Analysis. Communications in Computer & Information Science 420 (2014)
[7] S. Noel, and S. Jajodia, Metrics suite for network attack graph analytics, Cyber and Information Security Research Conference,(2014), p. 5-8.
[8] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, Measuring network security using dynamic bayesian network, ACM Workshop on Quality of Protection, (2008), p. 23-30.
[9] N. Poolsappasit, R. Dewri, and I. Ray, Dynamic security risk management using bayesian attack graphs. Dependable and Secure Computing, IEEE Transactions on 9 (2012)