ISSN: 2664-9640

Research on Forensic Analysis Method of Evidence Graph Model for Intrinsic Threat

Xianghua Liu

Wenzhou Polytechnic, Wenzhou, 325035, China

Abstract

Internal threat has become one of the main ways of network crime. Internal attack behavior has the characteristics of multi-step, camouflage, uncertainty and real-time dynamic change. Probability graph model can describe the causal dependence between multiple attack steps of the attack behavior, which is of great significance for analyzing complex multi-step attack behavior in forensics. In this project, a forensic analysis method based on the evidence graph model was proposed. Through the construction, evolution and clustering pruning process of the evidence graph, the attack status of the system was described completely in real time. Bayesian network is generated and calculated to identify the attacker, infer the attack path and reconstruct the attack scene. The main contents of this study include:(1) Construction and evolution of evidence graph for internal attack features; The system was described through real-time strong and weak evidence collection and inference Attack.(2) Based on the weak evidence inference of Hidden Markov Model, mining and effective correlation information from a large number of weak evidence;(3)Clustering and pruning of evidence graph based on graph Laplace spectrum analysis, and clustering of multiple attack steps associated with an attack process;(4) Generate probabilistic Bayesian network according to evidence graph and infer evidence. The research results of this project can be well applied to network crime analysis and forensics to improve the efficiency of forensics analysis.

Keywords

Network security; Network forensics; Attack graph; Evidence graph.

1. Introduction

The rapid development of network information technology and system has greatly changed the operation mode of enterprises, organizations and governments. But at the same time, the network attack technology also changes with each passing day, all kinds of security incidents emerge one after another. Among them, the attacks from internal malicious personnel often cause greater economic losses and more serious consequences than ordinary external attacks, which has become an important security problem faced by many governments, enterprises and organizations.

In 2010, Private Manning illegally downloaded a large number of classified documents and videos, burned them on CDs and took them out of the military base. Later, more than 90,000 Afghan war documents were exposed by WikiLeaks, which triggered a strong "earthquake" in the global political and security circles. In 2013, the "Prism Gate" incident of Snoden, the United States, leaked the information of the surveillance program of the United States, which also caused a great stir in the world. How to protect information assets from internal threats has attracted attention from all walks of life. At the same time, improving the ability to analyze and deal with internal threats after the fact has become a realistic problem to be solved.

Different from external attacks, internal attackers are authorized to access the internal network information system of the enterprise, and their attack behavior is camouflaged, and the trace of

ISSN: 2664-9640

attack is often more difficult to be detected. Malicious internal personnel can abuse their legal rights, under the cover of normal behavior to engage in illegal activities, conduct behavior camouflage; They can also use professional or social engineering methods to obtain other people's identity authentication information, impersonate legitimate users to enter other people's computers or data centers to steal confidential data, and carry out identity camouflage. In the face of disguised internal attackers, the access control policy faces the risk of failure because users launch attacks under normal permissions. However, traditional security protection means such as intrusion detection system IDS and firewall cannot monitor internal activities, so they cannot generate corresponding alarm and evidence data, which brings some challenges to the forensics analysis of internal threats.

Based on the analysis of the above background, oriented information system after the attack of forensic analysis and disposal requirements, in view of the internal threat multistep, camouflage and the uncertainty of observed events, this project proposes a forensic analysis technology based on evidence figure insider threat, to deal with the evidence, and evidence graph model is constructed to intuitive said the collected evidence, to improve the internal attack described the accuracy and completeness; Based on the evidence graph, we study a series of analysis and processing processes, cluster and prune the evidence graph, and find multiple attack steps in an attack that are correlated with each other. According to the Bayesian network to calculate the attack path, identify the malicious attacker and calculate the probability of possible attack events, and on this basis of forensics analysis, and finally form an effective method of evidence reasoning and attack scenario reconstruction. This method to analyze the potential risk in network in time, maintain the security of network system, and can forecast sudden attack, through a series of evaluation analysis, the effective prevention measures given the threat of network vulnerability, which can greatly improve the efficiency of network security event analysis forensics, threat to effectively deal with the internal attack, network security and information security field has a certain practical significance and application value.

2. Systematic research

Intrinsic threat based attack forensics involves the analysis of multi-source evidence data from the network, host and environment to identify malicious attackers and attack paths, and finally achieve the purpose of reconstructing attack scenes. Although the firewall and intrusion detection system have been deployed to detect and prevent the occurrence of attack, but these protection methods can not completely eliminate the threat of internal attack. Therefore, it is of great significance to study efficient post-analysis forensics technology, infer according to evidence, identify malicious attackers and attack paths, and reconstruct attack scenes.

Forensic technology involves the collection, preservation, analysis and presentation of evidence and other steps. This study focuses on the analysis and reconstruction of evidence in forensic technology. This project mainly focuses on the following challenges in network forensics analysis facing insider threats:

(1) internal threat is camouflage, attack process is often hidden under the normal behavior, therefore forensic analysis often need to deal with a lot of high noise data, the evidence from the collected data of the traditional safety devices and sensors, such as IDS alerts, often contain by normal behavior or other attacks has nothing to do with the attack caused by a large number of noise data, which identify the attacker from large amounts of information it is very difficult to reconstruct attack scenario.

(2) Internal threat is multi-step, and internal attack may include multiple evolving steps, involving a series of different hosts, and using different attack modes. In addition, the evidence information of the attack is often distributed in different evidence collection sources, and the

ISSN: 2664-9640

attack presented by each evidence collection source is only a part of the complex attack scenario. In order to fully infer the occurrence process of attack events and reproduce the attack scene, it is necessary to carry out correlation analysis on multi-source and heterogeneous data.

In the face of these challenges, the current forensic analysis techniques are often carried out in a manual and random way, which takes a lot of time and is prone to errors. Therefore, there is a growing demand for efficient, automatic and extensible forensic analysis techniques. In general, according to the characteristics of internal threats in network attacks, the research of this project designed an automatic and systematic way to efficiently analyze a large number of multi-source heterogeneous high-noise data, identify the attacker and relevant attack evidence, and reconstruct the attack scene.

This project proposes a forensics analysis method based on evidence graph to help forensics analysts find relevant evidence from a large number of attack data and discover associated attack scenarios. We propose a strong and weak evidence inference based on the Hidden Markov Model to process the collected evidence. On this basis, the construction method of evidence map is proposed. By clustering and pruning the evidence graph, the association between attack steps can be formed. Bayesian network was generated based on evidence graph to calculate attack path and event probability. The core part of this study is the construction and processing of evidence map, as well as the attack inference process.

This project studies the forensics analysis technology of internal threat events based on evidence graph. Figure 1 shows the forensics analysis and reasoning process diagram of this study. The specific research content includes the following four aspects:

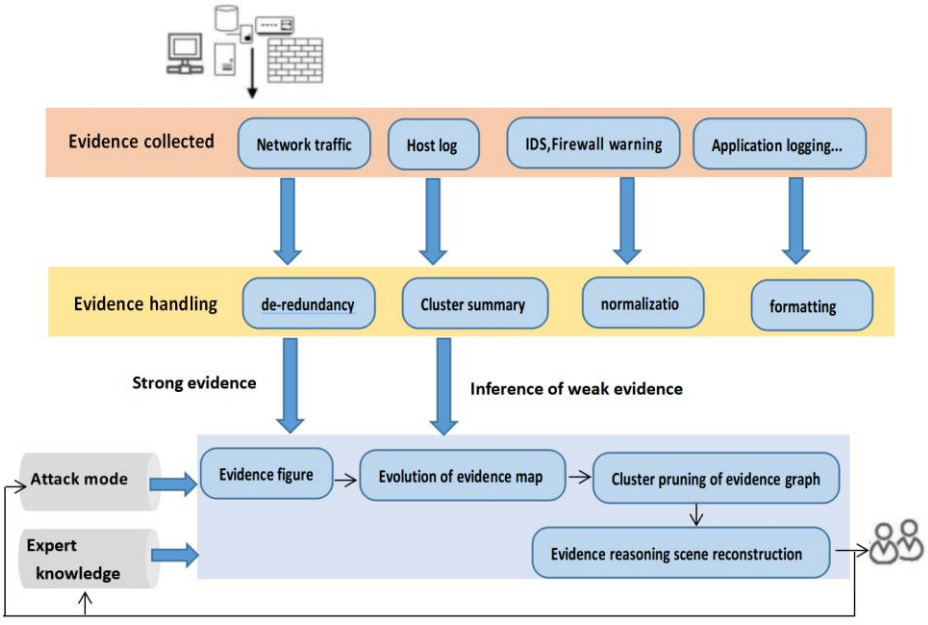

Fig. 1 Forensic analysis and reasoning process diagram based on evidence diagram

(1) Construction and evolution of evidence graph for internal attack features

Internal attack is multi-step, which is reflected in the fact that the internal attacker has enough time to observe, plan and implement the attack scheme, gradually attack the weaknesses of the system and achieve the attack target. This multi-step nature increases intra - attack forensics complexity. By modeling the attack process of the attack behavior and the target network, the evidence diagram can be used to describe the process of the attacker carrying out the attack step by step, improving the authority step by step, acquiring more resources and achieving the attack target.The evidence map can be used to describe the attack process of the attacker step by step. The evidence map is constructed according to the existing evidence, and the collected evidence is dynamically added into the evidence map in real time. To promote the evolution and improvement of the evidence map is the basis for further forensic analysis. The first part of

ISSN: 2664-9640

this project is: the construction and evolution of probabilistic evidence graph model for internal attack features, and the generation of evidence graph and the method of adding and updating evidence.

(2) Weak evidence inference based on Hidden Markov model

In forensic analysis, an event is an action that changes the state of an entity in the network. A malicious event is an event that is attacked by a malicious person. Therefore, we define evidence in forensic analysis as data that can provide information about the event in an attack scenario. On this basis, we divide the evidence collected in the forensics of insider threat into strong evidence and weak evidence.The second part of this project is to make certain assumptions on the missing evidence based on the known strong evidence and attack mode, and to infer the weak evidence based on the hypothesis, so as to find the evidence information related to an attack event from the inference results.

Clustering and pruning of evidence graph based on Laplace spectral analysis of graph

Due to the complexity and variety of evidence, the evidence map formed is often very large. How to find multiple steps related to an attack from a large evidence map is one of the main problems to be solved in intra threat forensics analysis. Clustering method is often used in data detection and processing. The basis of clustering is to combine similar or similar targets into groups. In the processing of evidence graph, we cluster on the basis of natural graph clustering that can form salient features among interrelated multi-step attacks, so that these multi-step attacks can be distinguished from other background noise and false positives warnings. The goal of clustering and pruning the evidence graph is to simplify the evidence graph and find the associated multi-step attack process.The third part of this project is to study a graph clustering and cutting method to find multiple attack processes associated with an attack in the evidence graph.

Attack process inference and scene reconstruction method based on Bayesian network

The last part of this project is to infer the attack event process and reconstruct the attack scene based on the generated and processed evidence map, and predict the probability of the occurrence of a certain type of attack event, so as to complete the forensics reasoning analysis process. According to the reasoning results, the attack mode library is updated with feedback, and the approximate optimal protection policy setting under the current state of the system is calculated to provide the administrator with reference and suggestions. Bayesian probability theory is often used to model uncertain phenomena. Probability refers to a series of varying degrees of probability ranging from certainty of occurrence to certainty of non-occurrence. Bayesian models combine expert knowledge with observational data and can be trained based on real-time observations. Modeling methods combining Bayesian probability theory with graph theory can create complex models containing a large number of interrelated hypotheses. Based on a series of related variables, a directed graph is used to represent the qualitative relationship and the local probability distribution, so as to express the quantitative information of the relationship strength. Therefore, this study uses Bayesian network to analyze the attack, infer the attack process and reconstruct the attack scenario. In addition, this project will also study the method of designing and calculating the real-time optimal security protection policy set of the system according to the results of forensic reasoning.

3. Implement the route

(1) A probabilistic attack graph model for inference of real time internal attack intention.

According to the analysis and definition of the evidence of internal attack, the definition of evidence graph is given, and on this basis, the evolution process of evidence graph is studied. We define the evidence graph as a directed acyclic graph, represented by a quaterple. Where: N represents the set of all nodes and L represents the set of all edges. Ln represents the

ISSN: 2664-9640

collection of attribute tags for nodes and LE represents the collection of attribute tags for edges. In the evidence diagram, each node Ni represents a host layer entity, and each edge Ei represents an evidence information.

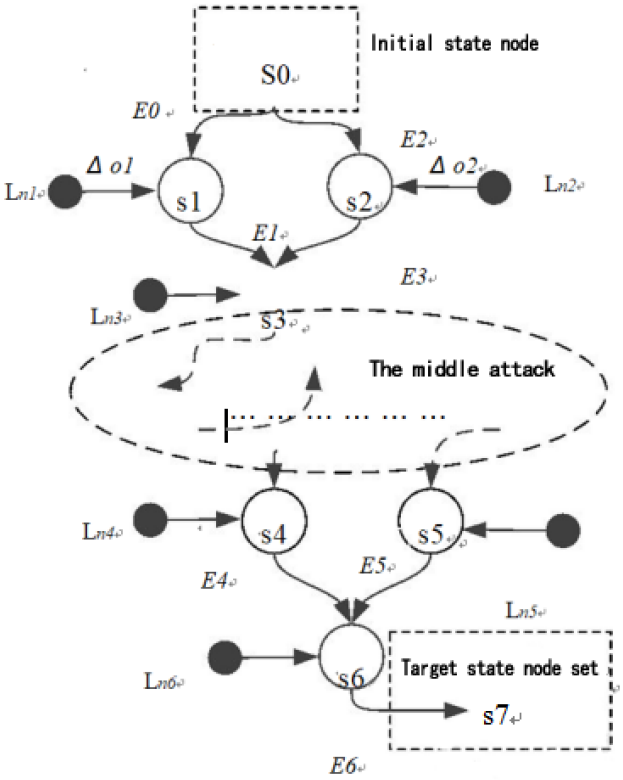

Fig. 2 Schematic diagram of probabilistic evidence diagram model

Each host layer entity attribute is represented by an ID identifying the entity and S representing the current state of the transformed entity which we have defined as four Attacker entities, Victim entities, Stepping entities and Related, i.e. S=(A, V, S, R). Tactivited indicates the start time of the entity state change, and TLatest indicates the most recent time of the state update[1].

The edge properties in the attack graph are represented by LE.=(W,R). Where W represents the weight of influence degree corresponding to this variable, that is, the influence degree of the attack represented by this edge on the connected nodes, i.e. the target host, if the attack is implemented, W =[0,1], such as the influence of a port scan attack W =0.2, and the influence of a buffer overflow attack W =0.8. R represents the credibility weight of this edge, that is, the probability between the observed evidence and the successful execution of this attack[2]. R ={0,0.5,1}, where r=1 indicates successful execution of the attack, and r=0 indicates failure of the attack. In other cases, r is set to 0.5.

According to the above definition, a schematic diagram of an evidence graph is shown in Figure 2 below.

Based on the defined evidence map, this study intends to use genetic algorithm to complete the evolution of the evidence map, complete the process of adding real-time observation evidence to the evidence map, and optimize the calculation of the influence of the evidence on the original evidence map. Genetic algorithm (ga) is on behalf of the problem may be a potential solution set of a population, whereas a population by a gene encoding a certain number of individuals, the original population is generated, according to the principle of survival of the fittest and the evolution, each subsequent generation evolution to produce more and more good approximate solution, in each generation, according to the individual problem domain size to choose the fitness of individuals, and by means of natural genetics, genetic operators of crossover and mutation, to produce on behalf of the new solution set of the population[3]. Through this process,

ISSN: 2664-9640

the influence of real-time evidence on the structure and parameters of evidence graph is calculated, and the problem of optimal evolution of evidence graph caused by the aggregation of new evidence is solved.

(2) Weak evidence inference based on Hidden Markov model

Some attacks can lead to a series of weak evidence, but the attacks themselves do not trigger an alarm and cannot be directly observed. Therefore, the purpose of the study is how to deduce implied aggressive behavior from a set of observational evidence, namely weak evidence. Hidden Markov Model (HMM) is a kind of Markov chain, whose states cannot be observed directly, but can be observed through the sequence of observation vectors. Each observation vector is represented by various states through some probability density distribution, and each observation vector is generated by a state sequence with corresponding probability density distribution. Hidden Markov model is a double stochastic process, the state transition process is unobserved, and the random process of observable events is a random function of the hidden state transition process.

A hidden Markov model is described by a quintuple $\lambda = (N, M, A, B, \pi)$ Among them:

$N = \{q1, \ldots, qN\}$ A finite set of states,

$M = (v1, \ldots vM)$ Is a finite set of observations;

$A = \{a_{ij}\}, a_{ij} = P(q_t = S_j \mid q_{t-1} = S_i)$ Is the state transition probability matrix;

$B = \{B_{jk}\}, b_{jk} = P(o_t = v_k \mid q_t = S_j)$ Represents the probability distribution matrix of observations;

$\pi = \{\pi_i\}, \pi_i = P(q_1 = s_i)$ Represents the initial state probability distribution[4].

Therefore, the process of inferring from observed events, namely weak evidence, can be summarized as the decoding problem in the Hidden Markov Model, namely, finding the state sequence with the highest possibility for a given model and sequence of observed values. In the construction of the Hidden Markov Model to solve the weak evidence inference problem, the selection of the initial probability distribution is generated by using the prior knowledge and the results of multi-sequence comparison. Viterbi algorithm is a grid structure algorithm similar to the forward algorithm. In this paper, based on the improved Viterbi algorithm, a dynamic programming algorithm is designed and implemented to solve the decoding problem of Hidden Markov Model. Through the process of initialization, recursion, termination and path backtracking of the algorithm, the optimal hidden sequence is calculated and the inference of weak evidence is completed.

(3) Clustering and pruning of evidence graph based on Laplace spectrum of graph

Clustering of graph structure means to select the best clustering to make the segmentation of graph achieve the goal of optimization. In the research of this project, we use the clustering method based on graph to cluster, and calculate the approximate optimal cutting edge of graph. In order to better represent the structural characteristics of the graph and extract information, we use the Laplacian representation matrix of the graph to calculate the graph of the evidence graph[5].

The evidence graph with the number of nodes n is expressed asGA=(V,E),The node set is v1,v2... ,vn., the set of edges is=v1,v2,... ,vn., The set of edges is $E \subseteq (V \times V)$,The weighted adjacency matrix of graph GA can be defined as:

$$A(i, j) = \begin{cases} w(i,j), if\ (i,j) \in E \\ 0, if\ (i,j) \notin E \end{cases}$$

Therefore, the degree matrix D can be defined as an N×N diagonal matrix, the values on the diagonal are d1,d2... The dn., one of them $d_i = \sum_{j=1}^{n} w(i, j)$ The demormalized Laplace

ISSN: 2664-9640

representation can be given by L equals D minus A. In this project, we use the following formula to calculate the normalized graph Laplace spectrum:

$$L_n := D^{-\frac{1}{2}} L D^{-\frac{1}{2}} = I - D^{-\frac{1}{2}} A D^{-\frac{1}{2}}$$

The clustering method based on graph Laplace spectrum consists of three stages. First, construct the Lapsus matrix representation of the graph. On this basis, the spectrum is calculated, and the Laplace spectrum of the graph is calculated by eigendecomposition. K feature vectors are selected, and the selected feature vectors are used to represent the graph as a subspace span, that is, the nodes in the graph are mapped to the space of low latitude. Finally, cluster points were established from the low-latitude space, and these points were corresponding to the original evidence map.

We designed a recursive spectral clustering algorithm to complete the clustering pruning process of the evidence graph. The first round of clustering firstly relies on the Laplace spectrum of the original evidence graph to find out the first group of clusters with obvious features and cut these clusters from the original evidence graph. After this operation, the original evidence graph changes into several relatively independent subgraphs. Thereafter, the Laplace matrix of all the large cluster graphs exceeding a certain threshold range k is recalculated, and the clusters with obvious features are extracted recursively in turn. Finally, the original evidence map was cut into multiple clusters, and the extracted clusters were used for further correlation analysis of the corresponding attack scenarios.

(4) Evidence reasoning process and method based on Bayesian network

It is very difficult to generate conditional probability table when constructing Bayesian network based on evidence graph. First of all, due to the uncertainty of the attacker's attack choice, even if all the events represented by the parent nodes of a node have occurred, it does not mean that the events represented by the node are bound to occur, because the attacker may choose to stop the attack, or the attacker may carry out the attack but the attack fails. Therefore, the conditional probability table value of this node needs to consider a series of causes. Yes, it is very difficult to generate and maintain the parameters of conditional probability table. For example, once the same attack behavior is found in other parts of the network, the possibility of the attacker choosing this attack method should be increased. However, in the structure of the evidence graph, it is difficult to distinguish the uncertainty of the choice of such an attacker from the values in the conditional probability table. Therefore, how to carry out this type of association update is a difficult problem in the construction of conditional probability table of Bayesian network.

Secondly, the analysis of internal attack events is different from the analysis of other attack types. Generally speaking, there is no way to learn CPT parameters on a large scale. The attack means and methods of the internal attackers are very flexible and always changing. Therefore, the generation of CPT parameters depends on fuzzy and subjective judgment. However, it is not feasible for experts to set CPT parameters for each Bayesian network model in practice. Most of the parameters should be generated automatically based on multi-source information, and can reflect the uncertainty of the attack event. Therefore, this study adopts the Bayesian network model to modularize the uncertainty and separate the processing to simplify the generation process of CPT parameters. In addition, due to the inherent inaccuracy of these parameters, modularization is adopted to reduce the sensitivity of CPT parameters of Bayesian network model and achieve better optimization.

According to the parameters set and the generated Bayesian network, the attack path and the probability of the attack event are calculated, and forensics reasoning is carried out. According to the result of reasoning, the optimal security protection strategy is calculated. The calculation of the optimal security protection strategy is a NP difficult task. If use violence algorithm, the

ISSN: 2664-9640

strategy of A total of 2 n values in different condition, its complexity is O (n * 2 (| S | + | | E | | + A)), which O (+ + | | A | | S | E |) for the value in each case, the target probability calculation algorithm complexity[6]. Therefore, on a given Bayesian network, through traversal of all security protection strategies, the probability difference between and is calculated, and the security protection measures with the maximum probability difference are selected. Finally, based on the above choices, the corresponding greedy algorithm is designed.

4. Implementation of network security assessment system

In view of the camouflage, multi-step, observation uncertainty and other characteristics of internal threats, this project aims to conduct dynamic and real-time attack event forensics analysis and disposal based on acquired and inferred evidence. This project intuitively represents the collected evidence through the construction of evidence graph model to improve the accuracy and completeness of description of internal attack state. Based on evidence graph, we study a series of analysis and processing processes, and conduct clustering and pruning of evidence graph to find multiple attack steps in an attack that are interrelated. According to the Bayesian network, the attack path is calculated, the malicious attacker is identified, the attack process is deduced, the attack scene is reconstructed, and the evidential reasoning process is completed. According to the inference results, the approximate optimal security protection strategy set calculation method satisfying certain cost restriction conditions is studied. How to make effective inferences from multi-source and heterogeneous weak evidence, and how to design evidence graph forensics model and Bayesian network algorithm with high reliability, high accuracy and high practicability under complex internal attack environment are the key scientific problems to be solved in this project.

Attack graph network performance is used to study its weakness to understand how attackers to attack, the attack jurisdictions, prior to its host permissions have agreed, to perform action to attack, use the web information of potential vulnerabilities, login to the host through remote login and other way, to get illegal information, in the local area network (LAN), each host connected, it gives the attacker to obtain other host permissions. In order to reduce the number of state space and to make the attack easily recognized by the computer, a simple graph model is used to construct the attack graph. To combine the generated attack graph with the attack model, the number of edges shown in the attack graph of the attacker's attack path may be unreachable. In order to eliminate the unreachable attack route, information nodes, the number of edges and attack nodes are defined in the attack graph to form the attack conditions. According to the simplification of calculation degree, the algorithm reduces the complexity and generates the attack graph according to the conditions. The algorithm of the attack graph is as follows:

Input:

AG // Network Attack Model

Where C represents the set of all nodes, including the target object and the original object C0.

//E represents the node that was attacked.

//R is the set of nodes and edgesOutput: $AG'(C' \cup C'_0, E', R')$

Procedure: graph_clean (AG)

initiate C', C'_0, E', and R' as empty sets.

bool mark[];

set each element of mark[] as false;

for each element c_0 in C_0,

push c_0 into node_stack;

mark[c_0]=true;

ISSN: 2664-9640

add c_0 into C' and C_0';
while(node_stack is not empty)
pop the top element of node_stack as w;
for each element e of Son(w);
if ! mark[e] and check(e),
mark[e]=true;
add e into E', and add all the edges of e into R';
for each element c of Son(e);
if ! mark[c],
mark[c]=true;
add c into C';
push c into node_stack;
return $AG'(C' \cup C_0', E', R')$

The algorithm first describes the attack node and several attack conditional nodes. When the attack path of the attacker is unreachable, the function in the algorithm is used to detect whether the condition is feasible. Under the premise that all attack nodes are feasible, the result is judged by the return value. Son(w) represents the support degree of W of the candidate set, indicating the probability of W appearing in the attack. If the attack node is not empty, the nodes will be added, and then whether mark[E] and mark[C] are true will be judged. If they are true, they will be put into the node stack. The above algorithm is based on the feature term and correlation algorithm to analyze the network weaknesses, network weaknesses are easy to form network vulnerabilities, attackers can launch attacks from it, detect the possibility of attack, which provides a foundation for the establishment of the attack model.

Attack model was set up by an attacker took advantage of network to be the process of the attacker to attack, the attacker because set the permissions on the gain in the network attack behavior, get permission after approval within the network resources are available on the host access, on this basis, according to attack condition, carry out purposeful action. After the network permission is passed, the attacker can launch the attack in two ways, which can be divided into indirect and direct. The main difference is whether the attacker has direct access to the target host, and whether gaining access to the attack is a series of actions that promote root access. According to the source access authority, source behavior, target behavior, attack behavior and a series of attack sequence reasoning, to carry out the establishment of attack graph and attack model.

Based on the establishment of attack graph algorithm and attack model, network information data transmission is established on this basis. Assuming that the virtual network is a local area network, the network design diagram is shown in Fig. 3.

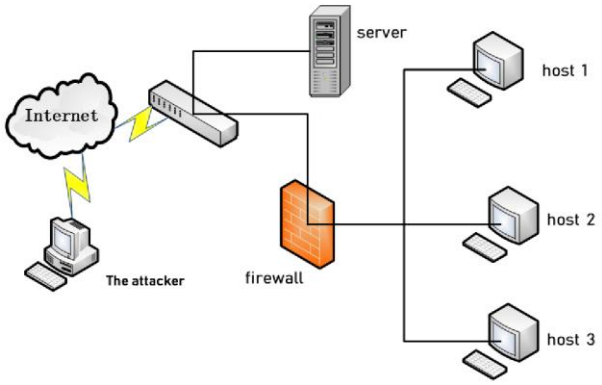

Fig. 3 Experimental topology structure diagram

ISSN: 2664-9640

The attacker obtains the information through the network cloud, according to the information in the switch, and then connects to the server and the user host. When the attacker accesses the user host, the firewall sets the permission to access, and detects the permission to access the command. Illegal access is effectively monitored through a series of traffic protocols and services run by the server. There are three hosts in the local subnet formed in Figure 1. Assuming that host 2 is an important business data server, it is highly likely to be attacked in the event of a system network crash. The ICMP configuration is set so that the host can be detected by the outside. The host can analyze the source address transmission of the data of the attacking host through ping command, data capture packet and other operations, so as to find out the attacker and what service the host runs in which network. Based on the vulnerability of the network to find the host, it launched an attack, to get some permissions to run on these hosts. Update the corresponding node detection in the calculated attack graph, and pass the updated calculated node and predictor.

Attackers attack is continuously increasing, will bring cumulative impact on the attacked, network security will not be guaranteed, set the code in the host permissions, the impact of the important confidential host is not to be underestimated, this assessment calculation and evaluation. The operating system of the network internal service environment of the tested attacker stored data packets, intercepted the packets, analyzed the data vulnerabilities, and found that the attack was contained in the data. Host log in scanning the environment, choose the target host network subnet, according to the IP address to determine the object, use Telnet to perform open and run the ping command to determine the various host server, according to the results, analysis of the data types in the host, after service system operation situation for the host permission after open application service command, and then use the host to the other in the target host.

In view of the camouflage, multi-step, observation uncertainty and other characteristics of internal threats, this project aims to conduct dynamic and real-time attack event forensics analysis and disposal based on acquired and inferred evidence. This project intuitively represents the collected evidence through the construction of evidence graph model to improve the accuracy and completeness of description of internal attack state. Based on evidence graph, we study a series of analysis and processing processes, and conduct clustering and pruning of evidence graph to find multiple attack steps in an attack that are interrelated. According to the Bayesian network, the attack path is calculated, the malicious attacker is identified, the attack process is deduced, the attack scene is reconstructed, and the evidential reasoning process is completed. According to the inference results, the approximate optimal security protection strategy set calculation method satisfying certain cost restriction conditions is studied. How to make effective inferences from multi-source and heterogeneous weak evidence, and how to design evidence graph forensics model and Bayesian network algorithm with high reliability, high accuracy and high practicability under complex internal attack environment are the key scientific problems to be solved in this project.

5. The conclusion

Network security risk assessment technology is mainly used to defend against network threats. It analyzes the huge data flow in the complex network system to defend against malicious attacks. Based on evidence figure to evaluate network forensics technology, attack graph analysis method is put forward first, and then with the general bayesian model to analyse, on the basis of the model using the combination of network vulnerability correlation analysis and algorithm, the effective evidence of network forensics is according to the figure and attack graph, combining algorithm for quantitative evaluation of the network vulnerability, to improve the network information to attack probability calculation and safety risk assessment.

ISSN: 2664-9640

The method model can monitor the attack trend and predict the attack means, give the objective analysis results combining with the network dynamics, and evaluate the network model in the real-time system. With the continuous development of the information security field, the practice of security assessment needs to be strengthened. Using less data monitoring to obtain a lower risk cost, the algorithm combined with machine learning processing can better fully show the attack path and attack means. In the next stage of work, the focus of reasoning on network vulnerability and evidence graph will be shifted to the implementation method, the efficient evaluation algorithm system will be designed, and the network forensics method architecture will be continuously improved in the network environment.

References

[1] China Internet Information Center. The 38th China Internet Development and Statistical Report [R]. Beijing: China Internet Network Information Center, 2016.
[2] Tian Zhihong, Yu Xiangzhan, Zhang Hongli, et al. Real-time Network Intrusion Forensics Method Based on Evidence Reasoning Network [J]. Chinese Journal of Computers, 2014(5) : 1184-1194.
[3] Zhang H, Yao D, Ramakrishnanvt N, Zhang Z B. Causality *reasoning about network events for detecting stealthy malware activities[J]. Computers & Security, 2016,58(C):180-198.*
[4] Gribaudo M, Iacono M, Marrone S. Exploiting Bayesian Networks for the Analysis of Combined Attack Trees[J]. Electronic Notes in Theoretical Computer Science, 2015,310(C):91-111.
[5]Poolsappasit N, Dewri R, Ray I. Dynamic Security Risk Management Using Bayesian Attack Graphs[J] . IEEE Transactions on Dependable and Secure Computing . 2012 (1)
[6] He J S, Chang C Y, He P, et al. Network Forensics Method Based on Evidence Graph and Vulnerability Reasoning[J]. Future Internet 2016,8(4):54.

The attached:

The authors introduce

Xianghua,LIU,Master of Software Engineering, graduated from Huazhong University of Science and Technology, working in Wenzhou Polytechnic,her research interests include Web applica tion security, data mining.