INFORMATION SECURITY RISK ASSESSMENT UNDER UNCERTAINTY USING DYNAMIC BAYESIAN NETWORKS

R. Sarala[1], M.Kayalvizhi[2], G.Zayaraz[3]

[1]Associate Professor, Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India
[2]Student, Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India
[3]Professor, Computer Science and Engineering, Pondicherry Engineering College, Puducherry, India

Abstract

The risk management process is the key task of every decision maker in an organization. This risk management process should be carried out periodically to review the security of the information assets in the organization. So if this process is to be efficient, the organization should first prioritize the information assets and should employ risk management procedure to avoid potential loss. But the uncertainty in the risk events and the additional tedious task of decision making under risk makes the risk management process inefficient. In this paper, a novel approach is presented; where Dynamic Bayesian Network models are constructed to identify multi stage attacks. The Dynamic Bayesian Network models help to detect the uncertain relationship associated with the risk event. The next task is inferring, where evidence is updated dynamically for the multiple time slices. Finally, a diagrammatic representation of the attack scenario and the constructed Dynamic Bayesian Network is shown to explain the effectiveness of the model in identifying multi stage attacks.

Keywords: *Information Security Risk Assessment, Information assets, Multi stage attacks, Uncertainty, Decision making*

--***--

1. INTRODUCTION

Every organization requires periodic risk assessment process which is essential for a healthy business process. In the current organization environment, dependence on electronic services has increased where all the business transactions are carried out electronically over internet. The fundamental precept of information security is to support the mission of the organization by securing its information assets. All organizations are exposed to uncertainties, some of which impact the organizations in a negative manner. The IT security management must be able to help their organizations understand and manage these uncertainties.

Managing uncertainties is a tedious task. Since resources are limited and the nature of occurrence of threats and vulnerabilities change rapidly, risks are impossible to mitigate. Therefore, a standard process is needed to ensure that all the threats and vulnerabilities which pose a risk to the organization are under control. This process needs to be consistent, repeatable and cost-effective and also reduce risks to a reasonable level. Security controls that are defined by the organization to ensure an adequate security level can be validated by a process called risk management. Besides this validation, risk management also defines strategy and goals in the area of information security. Risk is assessed by identifying the occurrence of threats and vulnerabilities and then calculating the threat likelihood. Unfortunately, risk assessment is a complex undertaking, usually based on uncertain information. There are many methodologies aimed at allowing risk assessment to be repeatable and give consistent results. One of the most difficult activities in the risk management process is to relate a vulnerability to a threat. Moreover, vulnerability-threat relation is a mandatory activity, since risk is defined as the exercise of a threat against vulnerability. This is called as pairing of vulnerability-threat. Not every threat-action/threat can be exercised against vulnerability. There are no standard list of available threats and their corresponding vulnerability as they would change fairly often. But it's inevitable for an organization to maintain the threat-vulnerability list and it could be used as a baseline. So a successful and effective risk management is the basis of successful and effective Information Security. Due to the reality of limited resources and nearly unlimited threats, a reasonable decision must be made concerning the allocation of resources to protect systems. Risk management practices allow the organization to protect information and business process commensurate with their value. The risk management should be consistent and repeatable for effective risk reductions. By enhancing a high quality risk assessment process, an effective information security risk management in the organization can be maintained.

1.1 Information Security Risk Management

The Risk management refers to the practice of identifying potential risks in advance, analyzing the risks and implement risk control techniques to mitigate the risks. Essentially, risk management is a periodic process. Lack of risk management can result in potential loss for organization as well as individuals.

The risk management techniques determine the risks that exist in the information assets and handle those risks in a way best-suited to the investment objectives. It is an ongoing process that continues through the business process. Risk Management includes risk identification, risk assessment, implementation of suitable control measure and finally monitoring the control measure. The risk management steps are updated over time, which also helps to mitigate new potential risk. It's the objective of risk management is to decrease the probability and impact of events adverse to the information assets.

1.2 Bayesian Belief Network

A Bayesian network consists of a directed acyclic graph and a set of local distributions. Each node in the graph is represented by a random variable. A random variable depicts an attribute, feature, or hypothesis about which the decision maker may be not certain. Each variable is randomly distributed which consists of jointly limited and collectively extensive possible values. That is, precisely one of the extensive possible values is or will be the distinct value, and the decision maker will be uncertain about which value it is. The graph represents direct casual dependence relationships between the nodes; the quantitative information is represented by local distributions about the strength of those dependencies. The local distributions and the graph together represent a joint distribution over the random variables denoted by the nodes of the graph.

Bayesian networks provide an elegant mathematical structure for modeling complicated relationships among random variables while keeping a relatively simple visualization of these relationships.

Bayesian Networks is known for being a powerful tool for performing decision making under uncertainty, but they have some drawbacks that hold back their application to complicated problems. As the technique is widely used, Bayesian Network's drawbacks became increasingly obvious. Bayesian Networks are not expressive enough for many real-time applications. More precisely, Bayesian Networks presume a plain attribute-value representation that is; each problem instance involves reasoning about the same fixed number of values, where only the evidence values changes from problem instance to problem instance.

1.3 Representing Uncertainty using Bayesian Network

Bayesian Belief Networks also known as Probability networks or Causal network are models for representing uncertainty in knowledge. Uncertainty arises in a variety of situations:

1. Uncertainty of knowledge
2. Uncertainty of the domain problem
3. Uncertainty in deriving conclusions
4. Uncertainty in available resources

Bayesian Belief Networks use probability theory to man-age uncertainty by explicitly representing the conditional dependencies between various information components. This provides an in-built graphical representation of the knowledge and also interactions among various sources of uncertainty.

1.4 Dynamic Bayesian Network

The Bayesian Belief network only works with variable results from a single slice of time. One possible and promising approach to deal with multistage attacks and with different time frame is to construct a Dynamic Bayesian Belief network (DBN). The Dynamic Bayesian network is an ideal model for combining existing information with new data and to infer future events. It is a graphical representation of cause and effect relationship within a problem domain. It provides a consistent semantics for representing uncertainty and provides graphical representation of interaction between causes and their effects.

A Dynamic Bayesian Network is made up with related time slices of fixed Bayesian networks. The nodes at a definite time can affect the nodes at a future time slice, but the nodes in the future time slice can not affect the nodes in the previous time slice. The spontaneous links across the time slices are indicated to as temporal links. The benefit of this gives the Dynamic Bayesian Network a definite direction of causality. For the convenience of computation, the variables in Dynamic Bayesian Networks are assumed to have a fixed number of states that the random variable has. Based on this, conditional probability tables can be calculated to express the probability of occurrence of each child node derived from conditions of its parent nodes. Thus, a DBN can illustrate the probabilities of one variable changing another variable, and also how each of the individual variables changes over time.

2. REALTED WORKS

Risk assessment based on Grey Relational analysis and Dempster –Shafer theory was proposed by Wei Miao [5]. The basic idea of the scheme was to establish an assessment index values and calculate the gray relational grades between the index values and the risk ratings.

Wang Lijian [6] introduced Bayesian network into information security risk assessment model which uses probabilistic reasoning to seek value at risk which is combined with expert knowledge.

Nayot Poolsappasit [7] proposed a BAG model to drive the decision process, which helps to better understand the casual relationships. The dynamic risk analysis helps to identify the weak spots in a network.

Alireza Tamjidyamcholo [9] proposed an InfoSecu risk Algorithm which can effectively reduce the risk derived from uncertain environments. First, the rate of the risk was assessed after which Genetic Algorithm was applied to reduce the scale of risk. An example is shown in which the Genetic Algorithm is effective in reducing the Information Security risks in an organization.

Artur Rot [4] presents the issue of one of the most signifi-cant stages of risk analysis which is IT Risk Assessment, especially focusing on chosen quantitative methods such as ALE method, Courtney method, Fisher's method, using survey research Information Security Risk Analysis Model (ISRAM) and other derived ratios.

Chunlu Wang [10] proposed a novel assessment approach that supports automatic attack graph generation based on the correlated vulnerability database and quantitative vulnerability assessment utilizing Bayesian attack graphs. And in order to facilitate the assessment and analysis process a Vulnerability Scanner is built using Open Vulnerability and Assessment Language that manually assigns probabilities to a Bayesian attack graph.

Nan Feng [1] provides a new way to define the basic belief assignment in fuzzy measure. An ISS index system is established and also the index weights are quantified based on which the evidential diagram is constructed. The Model also provides a method of testing the evidential consistency, which reduces the uncertainty derived from the evidence.

Suleyman Kondakci [8] presents a casual assessment model based on Bayesian Belief Networks to analyze and quantify information security risks caused by various threats sources. It also determines the joint risk propagation and the interdependence structures within the networks and information systems.

3. PROPOSED WORK

The main objective of the proposed work is to enhance the decision making process under uncertainty for effective risk assessment process in an organization. The priority of information assets varies from one organization to other. The organization must first prioritize their information assets and protect the one which imposes high potential loss. So after prioritizing the assets, risk management is done to calculate the risk of the assets. The main tedious task is reducing the uncertainties in the risk assessment process. The existing system focuses on reducing the uncertainty by modeling a Bayesian Network and then it infers to capture the potential attacks. But the main limitation in existing system is, it does not capture all the potential attacks that pose threat to the information assets. So a more efficient method is needed to capture all the attacks that occur in various time frames.

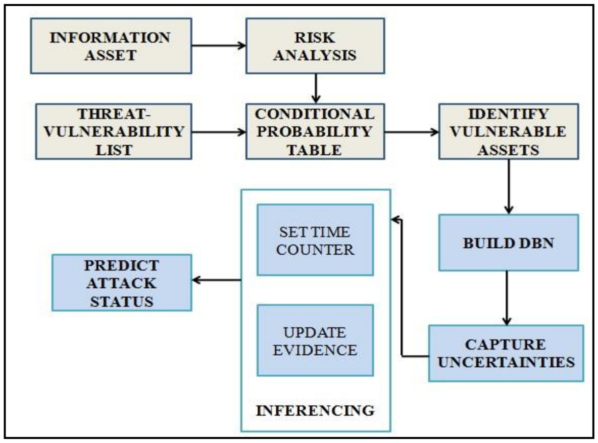


Fig -1: Proposed System Modules

The proposed work focuses on constructing a Dynamic Bayesian model where all the potential attacks that occur on different time frames are captured. Most of the potential attacks do not occur at a single stage or it won't be a direct attack. It takes multiple steps or stages for an attack to be successful. So by constructing a Dynamic Bayesian networks, the evidence can be inferred for different time frames, where the potential attacks can be captured.

When an attacker targets an Information system, the main aim is to damage the information assets or to get access to the assets. The attackers will be more conscious about their presence and might not want to get caught. So the attacker may cause a multistage attack where in the actual target of the attack is compromised by performing a series of attacks at different targets from different sources. The multi stage attacks distract the organization about the source of the attack. In each stage of attack, the attacker won't be a same person. It might be a multiple attackers targeting a single asset or single attacker targeting multiple assets. Therefore, the organization needs to be alarmed about all the possible ways that an attacker could intrude an asset. This is a more complex task; since the organization needs to deal with large amount of uncertain information which has an impact on decision process. Hence, considering all the above issues, a graphical model is built depicting all the possible ways of how an attacker will intrude an information asset by performing a multistage attack.

The Dynamic Bayesian Belief network is constructed which effectively reduces the uncertainty associated with a multistage risk event and the inference algorithm helps to infer about the multi stage attack. So a novel approach for inferring on multi attackers targeting single asset is proposed that provides a feasible and accurate prediction to the decision maker.

4. ATTACK SCENARIO

Let us look at an example as shown in the Fig -1.

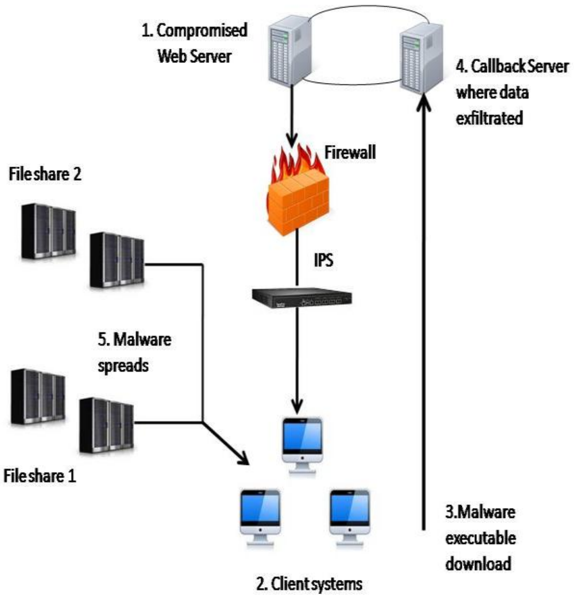

1. Compromised Web Server
4. CallbackServer where data exfiltrated
Firewall
Fileshare 2
IPS
5. Malware spreads
Fileshare 1
3.Malware executable download
2. Client systems

Fig -2: Water Hole Attack

The above attack scenario depicts about a sample water hole attack. In this attack, an attacker can intrude into the client systems and can inject a Trojan horse or any other malicious executable code in which by executing the malicious code in client systems, the attacker can intrude into the organizations system or steal any sensitive information, which pose some potential loss to the organization.

The attacker first exploits the system by compromising the web server by exploiting the vulnerability on the server software such as IIS. Once the web server is compromised, the attacker can wait for the client to hit a request. The attacker injects the malicious code by downloading it into the client system, once the client requests for a service from the web server. When the code is executed, the attacker gains access to the client system, where the attacker can download any data from the client system which is known as data exfiltration. Finally the malware spreads sidelong where the entire organization network becomes vulnerable.

The main advantage of dynamic Bayesian Network is that it predicts multiple time series into the future. For the above water hole attack, the Dynamic Bayesian Network can be created as follows.

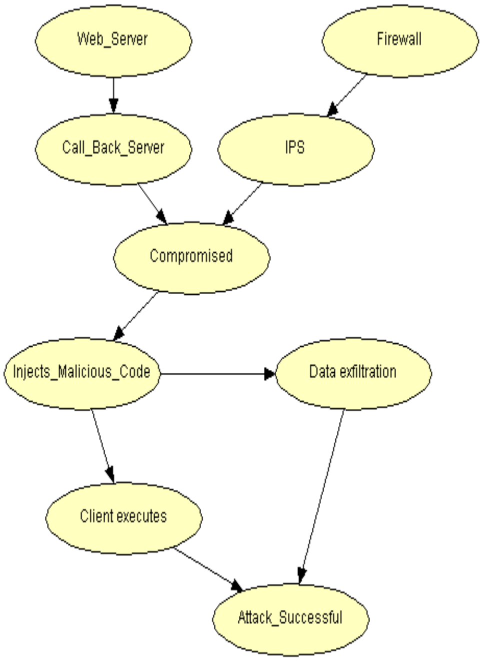


Fig -3: Dynamic Bayesian Model

After constructing the dynamic Bayesian network, inferencing is done where logical conclusions are done for the given attack. Here multistage attack architecture is developed where the whole process is simplified. Here time slices are initialized where the model can be inference on various time slices over the time period. And when new evidence arrives, it is updated dynamically for the corresponding time slice. Now, after constructing Dynamic Bayesian network the uncertain relations can be reduced by adding constraint nodes. In Fig.3, the node compromised is a constraint node, where if the web server is compromised, it will lead to an attack. SO by adding constraint nodes the uncertain factors associate with the assets can be reduced. The decision maker can predict the attack, by constructing a conditional probability table where the likelihood of each node is calculated. Table -1 show the CPT values for the above explained scenario.

Table -1: Conditional Probability Table

Nodes	Vulnerability exist	P(true)	P(False)
Web_Server	True	0.80	0.20
NFS_Shell_Attack	True	0.60	0.40
File_Server	True	0.70	0.30
Victim_Executes	False	0.20	0.80
Trojan Virus	True	0.70	0.30
Attack_Status	True	0.90	0.10

After calculating the conditional probability values, the inferencing is done. Junction tree inference algorithm is used to infer on the nodes, where the node with maximum probability value is likely to be exploited. The inferred nodes are represented in Fig.4.

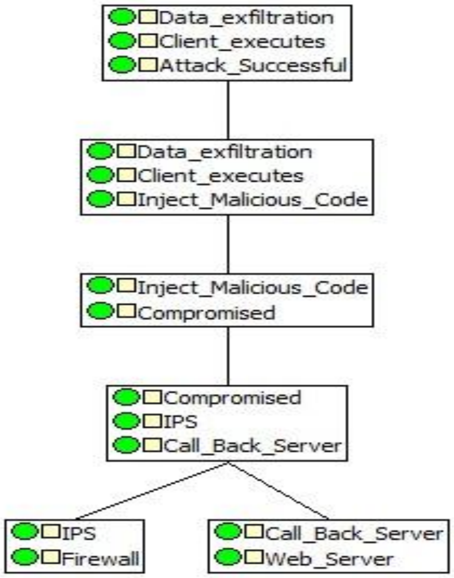
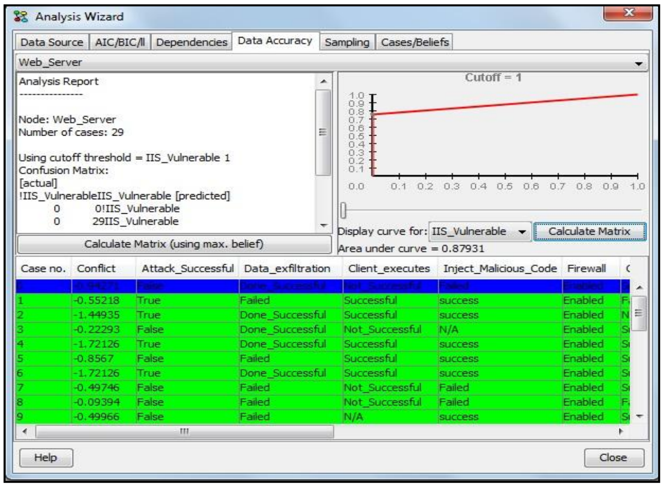


Fig -4: Junction Tree



```
Analysis Report
---------------

Node: Web_Server
Number of cases: 29

Using cutoff threshold = IIS_Vulnerable 1
Confusion Matrix:
[actual]
!IIS_VulnerableIIS_Vulnerable [predicted]
        0          0!IIS_Vulnerable
        0         29IIS_Vulnerable
```

Display curve for: IIS_Vulnerable

Area under curve = 0.87931

Case no.	Conflict	Attack_Successful	Data_exfiltration	Client_executes	Inject_Malicious_Code	Firewall	C
0	-0.94271	False	Done_Successful	Not_Successful	Failed	Enabled	S
1	-0.55218	True	Failed	Successful	success	Enabled	F
2	-1.44935	True	Done_Successful	Successful	success	Enabled	N
3	-0.22293	False	Done_Successful	Not_Successful	N/A	Enabled	S
4	-1.72126	True	Done_Successful	Successful	success	Enabled	S
5	-0.8567	False	Failed	Successful	success	Enabled	S
6	-1.72126	True	Done_Successful	Successful	success	Enabled	S
7	-0.49746	False	Failed	Not_Successful	Failed	Enabled	S
8	-0.09394	False	Failed	Not_Successful	Failed	Enabled	F
9	-0.49966	False	Failed	N/A	success	Enabled	S

Fig -5: Prediction Results

In Fig -5, the prediction results show that the Attack failed. Since the client_executes is not successful, the attack will be failed. The cutoff values show that the assets are in a safe state. If the cutoff value exceeds above one, the assets can be exploited. Thus the proposed work focuses on detecting multiple attacks that takes place on various time frames. The performance parameters for the model can be evaluated based on the amount of uncertainty reduced and accuracy of the inference algorithm used.

5. CONCLUSIONS

The traditional risk management process focuses on qualitative and quantitative analysis where the risk in the information assets is not reduced. The main hindrance in risk analysis is the uncertainty associated with each attack event and action. So by sorting the uncertain relationships, the decision maker can make reasonable decisions to prevent the attacks on information assets. To support this decision making process, modeling a Dynamic Bayesian networks will be effective in finding the uncertainties. So finally inferencing is done where the likelihood of occurrence of the attacks can be predicted. Thus the proposed work will be a promising approach to support the risk assessment process in every organization.

REFERENCES

[1]. Nan Feng, Minqiang Li, “An information systems security risk assessment model under uncertain environment,” Journal Applied Soft Computing, 2010.

[2]. Alma Cemerlic, Li Yang, Joseph M. Kizza “Network Intrusion Detection Based on Bayesian,” Proceedings of the Twentieth International Conference on Software Engineering & Knowledge Engineering, 2008.

[3]. Farhad Foroughi, “Information Security Risk Assessment by Using Bayesian Learning Technique,” Proceedings of the World Congress on Engineering, Vol I, 2008.

[4]. Artur Rot, “IT Risk Assessment: Quantitative and Qualitative Approach,” Proceedings of the World Congress on Engineering and Computer Science, 2008.

[5]. Wei Miao, Yanhua Liu, “Information system security risk assessment based on grey relational analysis and Dempster-Shafer theory”, International Conference on Mechatronic Science, Electric Engineering and Computer (MEC), August 2011.

[6]. Wang Lijian, Wang Bin, Peng Yengjun, “Research the Information Security Risk Assessment Technique based on Bayesian Network”, International Conference on Advanced Computer Theory and Engineering (ICACTE), 2010.

[7]. Nayot Poolsappasit, Rinku Dewri, Indrajit Ray, “Dynamic Security Risk Management Using Bayesian Attack Graphs”, IEEE Transactions on Dependable and Secure computing, 2012.

[8]. Suleyman Kondakci, “Network Security Risk Assessment Using Bayesian Belief Networks”, IEEE International Conference on Social Computing / IEEE International Conference on Privacy, Security, Risk and Trust, 2010.

[9]. Alireza Tamjidyamcholo and Rawaa Dawoud Al-Dabbagh, “Genetic Algorithm Approach for Risk Reduction of Information Security”, International Journal of Cyber-Security and Digital Forensics (IJCSDF), 2012.

[10]. Chunlu Wang, Yancheng Wang, Yingfei Dong, and Tianle Zhang, “A Novel Comprehensive Network Security

Assessment Approach", IEEE International Conference on Communications (ICC), 2011.

BIOGRAPHIES

R.Sarala is currently working as an Assistant Professor in the Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry, India. E-Mail: sarala@pec.edu

M.Kayalvizhi is currently pursuing master's degree programme in Computer Science and Engineering in Pondicherry Engineering College, Pondicherry, India. E-mail: kayalvizhi30@pec.edu

G.Zayaraz is currently working as a Professor in the Department of Computer Science and Engineering, Pondicherry Engineering College, Pondicherry, India. E-mail:zayaraz@pec.edu