www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 3 March 2015, Page No. 10977-10983

Intrusion Detection and Response Using Game Strategy And RRE Engine In Network Security

[1]Anuvarsha.G, [2]Rajesh kumar

Pg Scholar,
Sns College Of Technology,
Coimbatore.
Assistant Professor,
Sns College Of Technology,
Coimbatore

ABSTRACT

The security of the network reduces due to increase in the size of the network, there are many intrusion detection and intrusion response strategies which are carried on the basis to find and stop the intruders in the network such as local and global. Preserving the availability and integrity of networked computing systems in the face of fast-spreading intrusions requires advances not only in detection techniques and also in automated response techniques.

Here a new concept of game theory using Stackelberg game is introduced along with the RRE (response and recovery engine) to provide the automated response by using ART trees. In the intrusion detection system, the intruders can be found automatically by the IDS alerts but the response is to be provided by the manual process with is based on the time constraint, in order to overcome this drawback, the intrusion response system is provided with automation.

Keywords: Stackelberg game, ART trees, RRE engine, Markov Decision making, fuzzy rule set.

INTRODUCTION

The network is in the order of increasing size in day to day life hence the security of the network is to be affected in great manner. IP fragmentation, SMTP mass mailing, DoS attacks, flood attacks, spoofing, buffer overflow are some of the attacks that occur in the network. There is other serious threat in network considered to be Intrusion. Intrusion is an action or instance of intruding or an unwelcome visit or a set of actions aimed to compromise integrity, confidentiality, or availability, of a computing as well as networking resource. that is an intrusion on one’s privacy.in order to detect the intrusions the systems of intrusion detection, prevention and response systems are needed.

Incident handling [1] techniques are categorized into three MAIN classes. Intrusion prevention methods that take actions to prevent occurrence of attacks is of first. The intrusion detection systems (IDSes), such as Snort [2], which try to detect inappropriate, incorrect, or anomalous network activities[15] is of second. Finally, there are intrusion response techniques that take responsive actions based on received IDS alerts to stop attacks before they can cause significant damage and to ensure safety of the computing environment. There are many techniques that are introduced in such a way to improve the network security, in which the IDS (intrusion detection system) plays a major role. The intrusion detection algorithms are either based on identifying an attack signature or detecting the anomalous behaviour of the system. An IDS is a system or software to detect malicious or unacceptable system and network activity and to alert a systems administrator to this activity.

The IDS is used in order to improve the security of the network by finding suspicious activities, whether the network is of local or global, the security should be provided in a great manner. In the case of local network the size of the network is small hence the detection can be done with the incoming and outgoing data packets effectively. But in the case of the global network, the size increases hence the IDS is to be performed in the deep manner. Intrusion detection has been made automated in the network that finds whether the user is authorized or an intruder by the default characterises and details. As the network grows larger the intrusion response is also needed to be automated in order to provide the response as soon as possible.

Here the concept of RRE (Response and Recovery Engine) has come into account with the automation in the response. The RRE uses the ART trees i.e. The attack response trees in which the optimum response is provided by consequence nodes for an attack that detected by IDS.

Markov decision process is used to make the optimum decision for the intruders. In which is selects the optimum i.e. most suited response for the intruders based on their characteristics. The decision process is that deals with the true or false technique. This type of mechanism can be used in the case of the small scale networks.

In the case of the large scale networks, the markov decision process cannot be used in affective manner. Hence the fuzzy rule set is used to find out the values ranging from 0 to 1, it gives the optimum response based on the intermediate results of the intrusion detection system.

LITERATURE STUDY

There are many detection techniques used in the network in order to find the misbehaviour and the intruder . The unauthorized login and the usage of the network lead to loss of the information and the blocking of the information in the needed time.

EMERALD [11], a dynamic cooperative response system, introduces a layered approach to deploy monitors through different abstract layers of the network. Analysing IDS alerts and coordinating response efforts, the response components are also able to communicate with their peers at other network layers. AAIRS [12] provides adaptation through a confidence metric associated with IDS alerts and through a success metric corresponding to response actions. Though EMERALD, AAIRS and other offer great infrastructure for automatic IRS, they failed to balance intrusion damage and recovery cost.

LADS [5], a host-based automated defense system, uses a partially observable Markov decision process to account for imperfect state information; however, LADS cannot be applicable in general-purpose distributed systems due to their reliance on local responses and specific profile-based IDS. Balepin et al. [13] address an automated response-enabled system that is based on a resource type hierarchy tree and a directed graph model called a system map. Both LADS and the IRS in [13] can be exploited since none of them takes into account the malicious attacker's potential next actions while choosing response actions.

Lye and Wing [16] use a game-theoretic method to analyze the security of computer networks. The interactions between an attacker and the administrator are modelled as a two-player simultaneous game in which each player makes decisions without the knowledge of the strategies being chosen by the other player; however, in reality, IDSes help administrators probabilistically figure out what the attacker has done before they decide upon response actions, as in sequential games. AOAR [14], created by Bloem et al., is used to decide whether each attack should be forwarded to the administrator or taken care of by the automated response system. Thus the use of a single step game model makes the AOAR vulnerable to multistep security attacks in which the attacker significantly damages the system with an intelligently chosen sequence of individually negligible adversarial actions.

There are many limitations in the above techniques which that include more cost of the systems and the decisions and response are done by the predefined rules hence the intruder with a new strategy are cannot be guessed. To overcome the above disadvantages the concept of RRE engine is developed with the game theory.

Intrusion detection using RRE engine

A game-theoretic intrusion response engine, called the response and recovery engine is used. ARTs enable RRE to consider inherent uncertainties in alerts received from IDSes.

The security maintenance of computer networks is given by Stackelberg stochastic two-player game in which the leader and follower try to maximize their own benefits by taking optimal responses and actions. The system provides more security by the means of the game. The game type called sliding puzzle is used. The authentication process is made of with the double iteration, in the sense of both the password and the game are considered for the authentication purpose.

If the user or the client needs to access the server for information the server checks for whether the user is of registered. If the user is been registered then the client is to provide the unique user name and password which used for their registration. The client is asked to solve the game with the time limit in order to gain access to the server.

If the user needs to access the server for first time the server provides with registration process. The process includes the details of the user that to be filled for the security purpose and the process asks the user to solve the puzzle game that provided with the list of sequence hints which is to be followed by the user in order to solve the puzzle. The game will be provided by the administrator of the server. After the successful registration process the password and the game sequence are mailed to the client's email which makes the reduction of the remembrance of the password.

The login process is provided with the threshold value in which the client should complete the process in the specified value. If the value exceeds even the original user is considered to be an intruder. In the case the original user can make use of the mailed details for their safety access of the server.

The attack-response trees are designed offline by experts for each computing asset. It is important to note that, unlike the attack tree that is designed according to all possible attack scenarios, the ART model is built based on the attack consequences.

An attack-response tree's structure is expressed in the node hierarchy, allowing one to decompose an abstract attack goal (consequence) into a number of more concrete consequences called sub-consequences. A node decomposition scheme could be based on either OR or AND gate, where AND all of the sub-consequences, OR where any one of the sub-consequences, Some of the consequence nodes in an ART graph are tagged by response boxes that represent countermeasure (response) actions against the consequences to which they are connected.

Reciprocal interaction between the adversary and response engine in a computer system is a game in which each player tries to maximize his or her own benefit. The game is a finite set of security states that cover all possible security conditions that the system could be in. The system is in one of the security states at each time instant. RRE, the leader, chooses and takes a response action.

As the last step in the decision-making process in local engines, RRE solves the markov decision process (MDP) to find an optimal response action from its action space, and sends an action command to its agents that are in charge of enforcing received commands. The global engine's fuzzy controller is composed of the following elements:

1. A rule-base (a set of If-Then rules), which contains a fuzzy logic quantification of the experts linguistic description of how to achieve accurate global network-level security measure estimates.
2. An inference module, which emulates the experts' decision-making in interpreting and applying knowledge about how best to estimate the global network-level security measure values.
3. A fuzzification interface, which converts the controller inputs from local response engines into information that the inference mechanism can easily use to activate and apply rules.

A defuzzification interface is that which converts the conclusions of the inference mechanism into real number values as inputs to the game-theoretic intrusion response system to pick the cost-optimal response action.

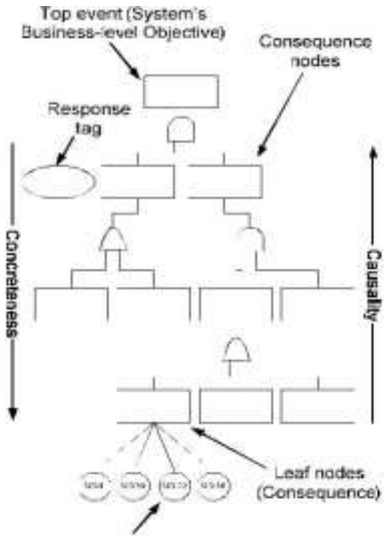
Attack Response Tree

Input: IP address

Output: attack response result R.

Steps:

1. ART graph construction initialization.
    a. An ART T encodes d in form of a tree.
    b. A node t in T without children is known as leaf node. Otherwise it is called as an internal node.
2. Read every attack countermeasure and construct under the relevant leaf node.
3. Receive the IDS alert from the local engine and perform the following.
    a. Read the IDS
    b. Match with the node n in T.
    c. Find the consequence, leaf node from T.
    d. Match the result with the higher level of leaf node
    e. Find the top event and response tag from ART.
4. Boolean values from the sub consequence are assigned to all nodes in the attack-response tree.
5. Return the result R.



<u>Procedure: Stahlberg game</u>

```
i/p- user details
O/p-authentication of user
while user is equal to new
do registration process
while user<> new
do login process
end while
end while
```

<u>registration process</u>

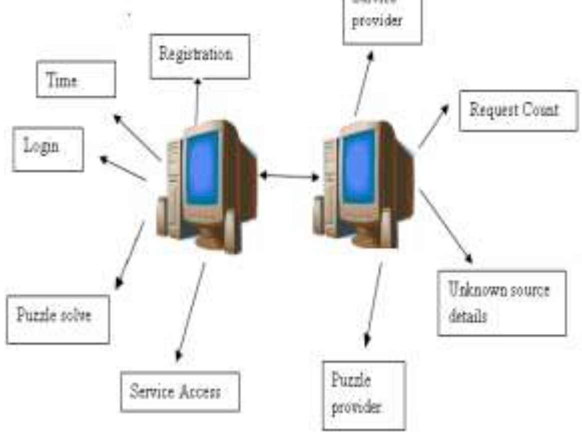
```
fill the details
if fields are not filled
fill all the details
else
all fields are filled
then
game solving process
end if
save and submit
```

<u>login process</u>

```
enter username and password
if username and password < > registered details
enter the correct username and password
else
username and password = registered details
submit
solve game
access details
```

<u>game solving process</u>

```
if game sequence < >  registered details
block the user
else
allow the user
end if
```



```
procedure:RRE engine
i/p- IDS, ART
o/p- final decision
read the IDS alert
if IDS alert=0 then
no intrusion
allow the user
else IDS alert=1 then
intrusion occurred
block the user from particular IP address
game solving process
if IP address is local host
select local engine process
else
select global engine process
end if
```

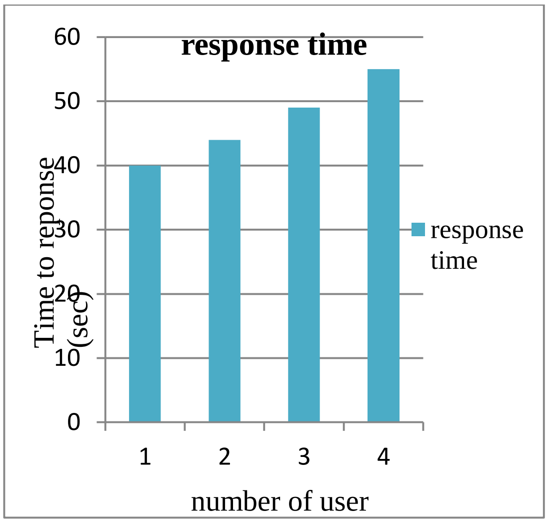
```
local engine process
get the IP address of user
check for the security state of the server
perform the markov decision with the output of art
if state> security
allow the user
else block the user
end if
send the result to RRE agent
RRE agent displays and responds the result to user.
```

```
Global engine process
Start process
get the IP address of user
check for the security state of the server
perform the fuzzy set analysis with the output of art
if state> security
allow the user
else block the user
endif
send the result to RRE agent
RRE agent displays and responds the result to user.
End process
```

As the client requests the server for access the IP that is address of the client is taken as the input for the Intrusion Detection System in which the input is taken as the Boolean values (0 or 1).

CONCLUSION

The proposed system improves the performance of intrusion response. Using the proposed system the system can yield the advantages as scalability in which the system can be applied to any global area and the security in the manner of prevention, detection and response for intrusion are increased. The user can access the server with easy accessibility. The server can be reached easily and the main importance and advantage of the game is that it avoids the password remembrance.



FUTURE WORK

The future work can be extended with the game type of wardrop game with individual player strategy and Node locality verification that is finding the exact location of the node by which the user logs to the server in the case of large networks. The Alert correlation tree and Attack verification tree by the server in order to correlate the alerted nodes and to verify the attack and the provided response to the user. With the advance the attack response selection tree is to be included in order to make the optimal response to the user. Game can be provided with the Graphical based click points based on the X-Y coordinates in order to provide the security in the enhance manner.

REFERENCE

[1] Devi Parikh, Tsuhan Chen,"Data Fusion and Cost Minimization for Intrusion Detection". IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 3, NO. 3, SEP 2008 pp 381-389

[2] Fu-Wen Chen and Jung-Chun Kao "Game-Based Broadcast over Reliable and Unreliable Wireless Links in Wireless Multihop Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 8, AUG 2013 pp 1613-1624

[3] Kai Hwang, Min Cai, Ying Chen,and Min Qin"Hybrid Intrusion Detection with Weighted Signature Generation over Anomalous Internet Episodes. "IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 4, NO. 1, JAN-MAR 2007. Pp 41-55

[4] Nicola Basilico, Nicola Gatti, Mattia Monga, and Sabrina Sicari2014 "Security Games for Node Localization through Verifiable Multilateration " IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 11, NO. 1, JAN / FEB pp 72-85

[5] O. Patrick Kreidl, and Tiffany M. Frazier, "Feedback Control Applied to Survivability: A Host-Based Autonomic Defense System." IEEE TRANSACTIONS ON RELIABILITY, VOL. 53, NO. 1, MAR 2004. pp. 148-166,

[6] Paul C. van Oorschot, Amirali Salehi-Abari, and Julie Thorpe" Purely Automated Attacks on PassPoints Style Graphical Passwords "IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 5, NO. 3, SEP 2010 pp 393-405

[7] Shi-Jay Chen and Shyi-Ming Chen,"Fuzzy Risk Analysis Based on Similarity Measures of Generalized Fuzzy Numbers." IEEE TRANSACTIONS ON FUZZY SYSTEMS, VOL. 11, NO. 1, FEB 2003. Pp 45-56

[8] Tatyana Ryutov, Clifford Neuman, Dongho Kim, and Li Zhou "Integrated Access Control and Intrusion Detection for Web Servers." IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 14, NO. 9, SEP 2003.pp 841-841

[9] Vivek Raghunathan and P.R. Kumar "Wardrop Routing in Wireless Networks ", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 8, NO. 5, MAY 2009 pp 636-652

[10] Zhenxin Zhan, Maochao Xu, and Shouhuai Xu"Characterizing Honeypot-Captured Cyber Attacks:Statistical Framework and Case Study" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 11, NOV 2013 pp 1775-118,

[11] P. Porras and P. Neumann, "EMERALD: Event Monitoring Enabling Responses to Anomalous LiveDisturbances," Proc. Information Systems Security Conf., 1997. pp.353-65,

[12] D. Ragsdale, C. Carver, J. Humphries, and U. Pooch, "Adaptation Techniques for Intrusion Detection and Intrusion Response System," Proc. IEEE Int'l Conf. Systems Man, and Cybernetics, 2000. pp. 2344-2349,

[13] I. Balepin, S. Maltsev, J. Rowe, and K. Levitt, "Using Specification- Based Intrusion Detection for Automated Response," Proc. Int'l Symp. Recent Advances in Intrusion Detection, pp. 136-154, 2003.

[14] M. Bloem, T. Alpcan, and T. Basar, "Intrusion Response as a Resource Allocation Problem," Proc. Conf Decision and Control, pp. 6283-6288, 2006

[15] saman a. zonouz, himanshu khurana, william h. Sanders and timothy m. yardley"RRE: a game-theoretic intrusion response and recovery engine" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, vol. 25, no. 2, february 2014 pp 395-406.

[16]K. Lye and J. Wing, "Game Strategies in Network Security," Int'l J. Information Security, vol. 4, pp. 71-86, 2005.