ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

RRE leverages Intrusion Response and Recovery Engine

Afroz Fatima
M.Tech Student
Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad
safa903222@gmail.com

SumeraJabeen
Assistant Professor
Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad
sumera06@yahoo.com

Ms.SalehaFarha
Head of the Department
Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad
salehafarha87@gmail.com

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 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, which try to detect inappropriate, incorrect, or anomalous network activities 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, 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 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, 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 profilebased IDS. Balepin et al.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 can be exploited since none of them takes into account the malicious attacker’s potential next actions while choosing response actions. Lye and Wing 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 , 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

EXISTING SYSTEM

The severity and number of intrusions on computer networks are rapidly increasing. Generally, incident-handling techniques are categorized into three broad classes. First, there are intrusion prevention methods that take actions to prevent occurrence of attacks, for example, network flow encryption to prevent man-in-the-middle attacks. Second, there are intrusion detection systems (IDSes), such as Snort, which try to detect inappropriate, incorrect, or anomalous network activities, for example, perceiving CrashIIS attacks by detecting malformed packet payloads. 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. So far, most research has focused on improving techniques for intrusion prevention and detection, while intrusion response usually remains a manual process performed by network administrators who are notified by IDS alerts and respond to the intrusions. This manual response process inevitably introduces some delay between notification and response,

DISADVANTAGES:

- Which could be easily exploited by the attacker to achieve his or her goal and significantly increase the damage.

- To reduce the severity of attack damage resulting from delayed response, an automated intrusion response is required that provides instantaneous response to intrusion.

PROPOSED SYSTEM

In this paper, we present an automated cost-sensitive intrusion response system called the response and recovery engine (RRE) that models the security battle between itself and the attacker as a multistep, sequential, hierarchical, non zero sum, two-player stochastic game. In each step of the game, RRE leverages a new extended attack tree structure, called the attack-response tree (ART), and received IDS alerts to evaluate various security properties of the individual host systems within the network.

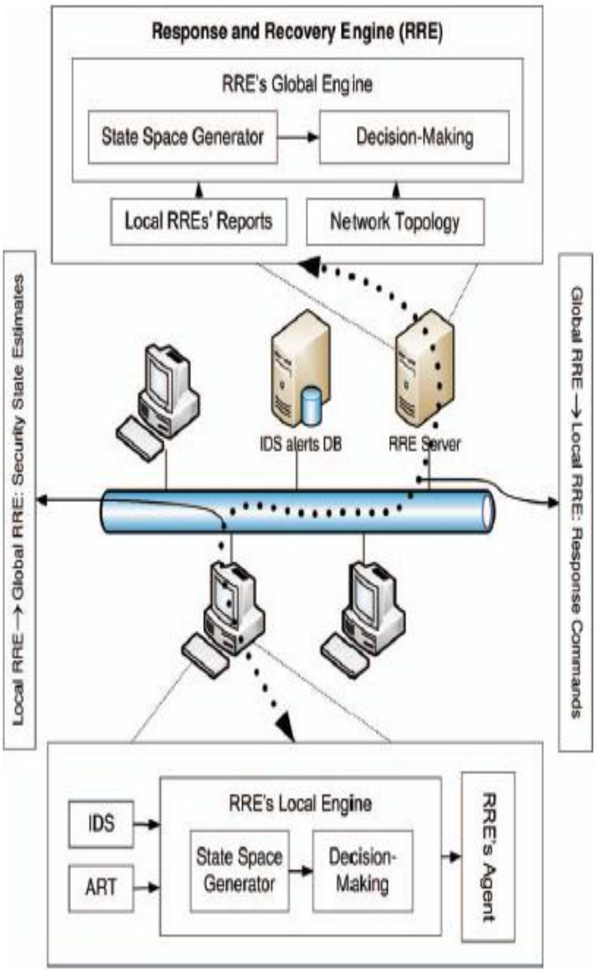
ARTs provide a formal way to describe host system security based on possible intrusion and response scenarios for the attacker and response engine, respectively. More importantly, ARTs enable RRE to consider inherent uncertainties in alerts received from IDSes (i.e., false positive and false negative rates), when estimating the system’s security and deciding on response actions. Then, the RRE automatically converts the attack-response trees into partially observable competitive Markov decision processes that are solved to find the optimal response action against the attacker, in the sense that the maximum discounted accumulative damage that the attacker can cause later in the game is minimized.

ADVANTAGES:

- Improves its scalability for large-scale computer networks, in which RRE is supposed to protect a large number of host computers against malicious attackers.

- Finally, separation of high- and low-level security issues significantly simplifies the accurate design of response engines.

SYSTEM ARCHITECTURE:



IMPLEMENTATION

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.

The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Automatic CMDP Generation:-

To generate the CMDP model, RRE analyzes the networktopology input to find out about the set of known systemvulnerabilities and individual host computers, i.e., privilegedomains. Given the set of system vulnerabilities, theconnectivity matrix is updated accordingly to encodeadversarial paths only. In particular, RRE automaticallygenerates a CMDP by traversing the connectivity matrixand concurrently updating the CMDP. First, RRE createsthe CMDP's initial state ð_Þ and starts the CMDP generationwith the network's entry point (Internet) node in theconnectivity matrix. Considering the connectivity matrix asa directed graph, RRE runs a depth-first search (DFS) on thegraph. While DFS is recursively traversing the graph, itkeeps track of the current state in the CMDP, i.e., the set ofprivileges already gained through the path traversed so farby DFS.

Multi-objective System Security Reward Function:-

Localengines send their local security estimates, i.e., rootnode probabilities _g of their ART graphs, to the RRE server.RRE considers the network's global security as a multi-objectivereward function for the response selectionprocedure. Each objective is represented by a specificsystem-level security property, and quantified by the _gvalues, which are calculated in the local engines. In ourmulti-objective game scheme, there is usually not a singlesolution that simultaneously minimizes each objective to itsfullest. In each case, we are looking for a solution for whicheach objective has been optimized to the extent that if we tryto optimize it any further, then the other objective(s) willsuffer as a result. RRE makes use of a fuzzy-logic basedcontroller that merges the involved objective functionvalues using an information fusion algorithm according tothe network security definition, and consequently, result ina single scalar reward value.

Fuzzy logic is a form of multi-valued logic derived fromfuzzy set theory to deal with reasoning that is approximaterather than precise. In contrast with binary sets whichfollow the binary logic, the fuzzy logic variables may have amembership value of not only 0 or 1. Just as in fuzzy settheory, with fuzzy logic, the set membership values canrange (inclusively) between 0 and 1, and the degree of truthof a statement, for example, The network is currently secure.,can range between 0 : false and 1 : true and is notconstrained to only two digital values as in classicpropositional logic. In particular, RRE calculates the globalnetwork security level, i.e., the truth degree of the "Thenetwork is currently secure" predicate, using a fuzzy control system that analyzes analog input values in terms oflogical variables (system-level security properties) fromlocal response engines that take on continuous values _g,and produces the network-level security measure values.

The global engine's fuzzy controller is composed of thefollowing four elements:

1. A rule-base (a set of If-Then rules), which contains afuzzy logic quantification of the experts linguisticdescription of how to achieve accurate globalnetwork-level security measure estimates.
2. An inference module, which emulates the experts'decision-making in interpreting and applyingknowledge about how best to estimate the globalnetwork-level security measure values.
3. A fuzzification interface, which converts the controllerinputs _g from local response engines intoinformation that the inference mechanism can easilyuse to activate and apply rules.

4. A defuzzification interface, which converts theconclusions of the inference mechanism into realnumber values as inputs to the game-theoreticintrusion response system to pick the cost-optimal
response action.

RELATED WORK

EMERALD , a dynamic cooperative response system, introduces a layered approach to deploy monitors through different abstract layers of the network. Analyzing IDS alerts and coordinating response efforts, the response components are also able to communicate with their peers at other network layers. AAIRS provides adaptation
through a confidence metric associated with IDS alerts and through a success metric corresponding to response actions. Although EMERALD and AAIRS offer great infrastructure for automatic IRS, they do not attempt to balance intrusion damage and recovery cost.

LADS , a host-based automated defense system, uses a partially observable Markov decision process to account for imperfect state information; however, LADS is not applicable in general-purpose distributed systems dueto their reliance on local responses and specific profilebased IDS. Balepin et al.address an automatedresponse-enabled system that is based on a resource typehierarchy tree and a directed graph model called a systemmap. Both LADS and the IRS in can be exploited by theadversary, since none of them takes into account themalicious attacker’s potential next actions while choosingresponse actions.

Game theory in an IRS-related context has also beenutilized in previous papers. Lye and Wing use a gametheoreticmethod to analyze the security of computernetworks. The interactions between an attacker and theadministrator are modeled as a two-player simultaneousgame in which each player makes decisions without theknowledge of the strategies being chosen by the other player;however, in reality, IDSes help administrators probabilisticallyfigure out what the attacker has done before theydecide upon response actions, as in sequential games. AOAR, created by Bloem et al., is used to decide whethereach attack should be forwarded to the administrator ortaken care of by the automated response system. Use of asingle-step game model makes the AOAR vulnerable tomultistep security attacks in which the attacker significantlydamages the system with an intelligently chosen sequence ofindividually negligible adversarial actions.

CONCLUSIONS

A game-theoretic intrusion response engine, called the response and recovery engine, was presented. We modelled the security maintenance of computer networks as a Stackelberg stochastic two-player game in which the attacker and response engine try to maximize their own benefits by taking optimal adversary and response actions, respectively. Experiments show that RRE efficiently takes appropriate countermeasure actions against ongoing attacks that save system damage and intrusion response cost compared to existing static and dynamic IRS solutions.

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.

REFERENCES

[1] B. Foo, M. Glause, G. Howard, Y. Wu, S. Bagchi, and E. Spafford, Information Assurance:

Dependability and Security in Networked Systems. Morgan Kaufmann, 2007.

[2] R. Rehman, Intrusion Detection Systems with Snort. Prentice-Hall, 2003.

[3] F. Cohen, "Simulating Cyber Attacks, Defenses, and Consequences," http://all.net/journal/ntb/simulate/simulate.html, 1999.

[4] S.A. Zonouz, H. Khurana, W.H. Sanders, and T.M. Yardley, "RRE: A Game-Theoretic Intrusion Response and Recovery Engine," Proc. IEEE/IFIP Int'l Conf. Dependable Systems and Networks (DSN), pp. 439-448, 2009.

[5] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the Slammer Worm," IEEE Security and Privacy, vol. 1, no. 4, pp. 33-39, July/Aug. 2003.

[6] B. Schneier, Secrets and Lies: Digital Security in a Networked World. John Wiley & Sons, 2000.

[7] A. Valdes and K. Skinner, "Adaptive, Model-Based Monitoring for Cyber Attack Detection," Proc.Recent Advances in Intrusion Detection, pp. 80-92, 2000.

[8] C. Kruegel, W. Robertson, and G. Vigna, "Using Alert Verification to Identify Successful Intrusion Attempts," Information Processing and Comm., vol. 27, pp. 220-228, 2004.

[9] G. Owen, Game Theory. Academic Press, 1995.

[10] J. Filar and K. Vrieze, Competitive Markov Decision Processes. Springer-Verlag, 1997.

[11] S. Hsu and A. Arapostathis, "Competitive Markov Decision Processes with Partial Observation," Proc. IEEE lnt'l Conf. Systems, Man and Cybemetics, vol. 1, pp. 236-241, 2004.

[12] L. Kaelbling, M. Littman, and A. Cassandra, "Partially Observable Markov Decision Processes for Artificial Intelligence," Proc. German Conf. Artificial Intelligence: Advances in Artificial Intelligence, vol. 981, pp. 1-17, 1995.

[13] E. Sondik, "The Optimal Control of Partially Observable Markov Processes," PhD thesis: Standford Univ., 1971.

[14] R. Bellman, Dynamic Programming, Princeton Univ. Press, 1957.

[15]D.F.Jenkins and K.M.Passino, "An Introduction to NonlinearAnalysis of Fuzzy Control Systems," J. Intelligent and FuzzySystems, vol. 7, no. 1, pp. 75-103, http://dl.acm.org/citation.cfm?id=1314668.1314674, Jan.1999

Authors:

Afroz Fatima, Presently, she is pursuing her Masters in Computer Science fromShadan Women's College of Engineering and Technology, Khairatabad, Hyderabad, T.S, India. Her research interests include image processing, and data mining.

Mrs. SumeraJabeenhas completed B.Tech (Information Technology) from JNTUH, M.Tech (Computer Science Engineering) from JNTUH. She is having 3 years of experience in teaching field. Currently, she is working as an Assistant Professor of CSE Department in Shadan Women's College of Engineering and Technology, Hyderabad, T.S, India.

Ms. SalehaFarha did her M.Tech in Computer Science and Engineering from Jawaharlal Nehru Technological University, Hyderabad. She did her B.Tech in Computer Science and Engineering from the same university, Hyderabad. She is working as an Associate Professor and HOD in CSE department.