RRE: Network intrusion detection and Game-Theoretic for response strategy for automated response.

Diksha Jadhav, Neha Patil, Parmeshwar Deshmukh, Rohit Patil, Rucha Dixit

Abstract— **In the world of fast-spreading intrusions requires advance technologies not only in detection algorithms, but also in automated response techniques for preserving the availability and integrity of networked computing systems. A new approach to automated response is made called the response and recovery engine (RRE). The response and recovery engine creates a game-theoretic response strategy against opponents in a two-player Stackelberg stochastic game. The RRE makes use of attack-response trees (ART) to analyze undesired system-level security events within host computers and their countermeasures. Boolean logic is used to combine lower level attack consequences. The RRE also accounts for the uncertainties in alert notifications during intrusion detection. The RRE then chooses optimal response actions after solving a partially observable competitive Markov decision process. It is automatically derived from attack-response trees. In order to support network-level multi-objective response selection and considering possibly conflicting network security properties, fuzzy logic theory is used to calculate the network-level security metric values, i.e., security levels of the system's current state and probable future states in each stage of the game. In particular, inputs to the network-level game-theoretic response selection engine, are first given into the fuzzy system that is in charge of a nonlinear inference and quantitative ranking of the possible actions using its predefined fuzzy rule set. Consequently, the optimal network-level response actions are chosen through a game theoretic optimization technique. Experimental results show that the RRE, using Snort's alerts can protect large number of networks for which attack-response trees have more than 500 nodes.**

Index Terms—**Intrusion Detection System (IDSes), Attack Response Tree (ART), Response and Recovery Engine (RRE),Fuzzy Logic, Markov decision processes.**

I. Introduction

The severity and variety of intrusions on computer networks are increasing fast. This is the reason why preserving the provision and integrity of networked computing systems has turned out to be one of the prime necessity. If we divide the incident handling into three wide classes then First, there are intrusion prevention methods that take actions to prevent occurrence of attacks, for instance, network flow encryption to prevent man-in-the-middle attacks. Secondly, there are intrusion detection systems (IDSes), Snort is one among the examples, which try to detect incorrect, inappropriate, or anomalous network activities. These activities could be like, perceiving CrashIIS attacks by detecting ill-shapen packet payloads. Finally, there exists intrusion response techniques those are responsible for taking responsive actions based on IDS alerts received, to stop attacks before they can cause any sort of damage and to ensure safety of the computing environment.

As far as it is concerned, most researches have focused on improving techniques for intrusion prevention and detection, and intrusion response usually remains a manual process performed by network administrators. These network administrators get notified with IDS alerts and then they manually respond to the intrusions. This manual response process introduces some delay between notification and response, which could be easily achieved and exploited by the attacker and may significantly increase the damage. And this delay cannot be avoided if the response is manual. Therefore, to decrease the severity of attack damage resulting from delayed response, an automatic i.e. non-manual intrusion response is needed that provides quick response to intrusion. This simply means there is a requirement of advance technologies not only in detection algorithms, but also in response techniques and this advancement could be achieved by an integration automated response techniques.

We present an automated cost-sensitive intrusion response system called the response and recovery engine (RRE). RRE models the security battle between itself and the attacker. It is the resemblance of multistep, sequential, hierarchical, non zero sum, two-player stochastic game as in where the RRE and the attacker are the two opponents.

In every step of the game, RRE is compounded with a new extended attack tree structure, called the attack-response tree (ART), and received IDS alerts. These alerts evaluate various security properties of the individual host systems within the network.

ARTs give a formal way to describe host system security based on possible intrusion and response scenarios for the attacker and response engine, respectively. Mainly, ARTs enable RRE to consider inherent uncertainties in alerts received from IDSes (i.e., false positive rates and false negative rates), when it has to estimate the system's security and deciding on response actions.

Then, the Markov decision processes are used i.e. RRE automatically converts the attack response trees into partly observable competitive Markov decision processes that are solved to find the optimal response action against the attacker, that means the maximum discounted accumulative damage that the attacker can cause later in the game is minimized. It is worthy that despite the mathematical cost minimization in RRE that itself requires certain time to complete in practice, RRE's ultimate objective is to reduce intrusion response costs

Diksha Jadhav, Computer Science, SPPU/JSCOE, Pune, India, +919422943303.
Neha Patil, Computer Science, SPPU/JSCOE, Pune, India, +919527764179.
Parmeshwar Deshmukh, Computer Science, SPPU/JSCOE, Pune, India, +919552447483.
Rohit Patil, Computer Science, SPPU/JSCOE, Pune, India, +918600869083.
Rucha Dixit, Computer Science, SPPU/JSCOE, Pune, India.

and the system damages due to occurring attacks compared to existing intrusion response solutions.

This is the game theoretic approach, the RRE adaptively adjusts its behavior according to the attacker's probable future reactions, and thus prevents the attacker from causing significant damage to the system by taking an intelligently chosen sequence of actions. To deal with security issues with different granularity, RRE's two-layered architecture consists of local engines, that resides in individual host computers, and the global engine, that resides in the response and recovery server and takes the decision on global response actions when the system is not recoverable by the local engines.

RRE employs a fuzzy control-based technique that can take into account several different specific properties and business objective functions simultaneously. The RRE calculates quantitative scores of the possible network-level response actions using its previously defined fuzzy rule set. The fuzzy rule set is defined using fuzzy numbers, and hence, various input parameters can take on qualitative values such as high or low ranging between 0 to 1; therefore, the real-world challenge that accurate well defined values of the involved parameters those are not always known, is addressed completely. RRE extends the state of the art in intrusion response in certain fundamental ways. We demonstrate that RRE is computationally efficient for large networks via prototyping and experimentation, show that it is practical by studying commonly found power grid critical infrastructured networks. However, we believe that RRE is widely applicable to all types of networks.

II. Motivation

For a large network of computer system is deployed in an area, there are number of systems. The network is increasing in size daily life hence the security of the network is to be affected in great manner. IP fragmentation, Simple Mail Transfer Protocol (SMTP) mass mailing, DoS attacks, flood attacks, spoofing, buffer overflow are some of the attacks that occur in the network. The other serious threat in network considered is intrusion. The systems are prone to intrusion. The need to overcome problem of security maintenance of computer networks is one of the motivations

The main aim is to detect these intrusions and provide an appropriate counter-measure actions against ongoing attacks that save system damage and provide proper response to the intruders.

Intrusion response usually is considered to be a manual processes performed by network administrators who are notified by IDS alerts and respond to the intrusions. The manual response process introduces some delay between notification and response, now this makes the problem persist again as the response can be easily exploited by the attacker. Genetic algorithm used for IDS were the most efficient techniques for intrusion alerts but along with that proper automated response was the main motivation.

RRE is given the preference as it could satisfy all the requirements, to be specified we get the technique for automated response with the reduction of intrusion response cost and intrusion response time.

III. Purpose

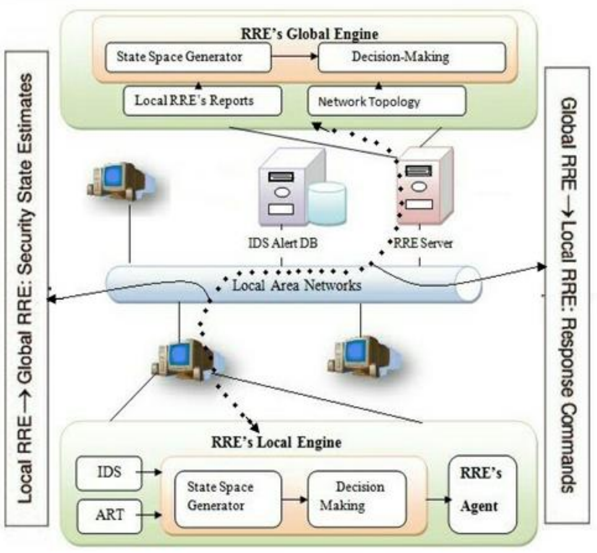
- There exist many intrusion detection systems those act of detecting actions that attempt to compromise the confidentiality, integrity or availability of a computer resource can be referred as intrusion detection.
- But these intrusion detection system have certain issues to be handled. There is a need to overcome these problems. Hence we preferred RRE as it not only overcomes all the problems regarding IDS as well as focuses on the automated response.
- In the intrusion detection system, the attacker can be found automatically by the IDS alerts but the response is to be provided by the manual response process with is based on the time constraint, in order to overcome this drawback, the intrusion response system is provided with automation. So we go for RRE.
- Unlike other strategies for the response which may contain manual methods, RRE implies a game theoretic response strategy which clarifies the basic mechanism for the automated response.
- There is also need of scalability for the intrusion detection systems and also the response systems. RRE is so designed that it can be applied to any global area and the security in the manner of prevention, detection and response for intrusion are increased.

IV. Scope

- RRE has wide applicability to all kinds of networks this is because of the provision of the solution to every possibility which makes the implementation of RRE universal.
- The future work can be extended with the game type of war drop 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.
- Moreover the verification of attack and the responses to the user can be done by using Alert correlation tree and Alert verification tree. This will enhance the technique of giving optimal response which will lead the response close to the accuracy.
- The implementation of RRE has been done on a very basic IDS i.e. the snort IDS, whereas in further implementations of high level and more profound IDS with more signified algorithms can be done.

V. Proposed System

Here, we present an automated cost sensitive intrusion detection response system called the response and recovery engine (RRE) that models the security battle between the intruder and itself as a multistep, sequential, hierarchical, non zero sum, two player stochastic game. In every step of the game, RRE leverages a new extended attack tree structure, called the attack-response tree (ART), and received intrusion detection system (IDS) alerts to evaluate various security properties of the individual host systems i.e. end user, within the network. ARTs provide a formal way to describe host system security based on probable intrusion and response scenarios for the attacker and response engine, respectively. Mainly, ARTs enable RRE to consider inherent uncertainties in alerts received from IDSes (i.e., false positive and false negative rates), when guessing the system's security and deciding on response actions. Then, the RRE automatically converts the ARTs into partially observable competitive Markov decision processes that are solved to find the optimal response action against the attacker, that means the maximum discounted accumulative damage that the attacker can cause later in the game is minimized.

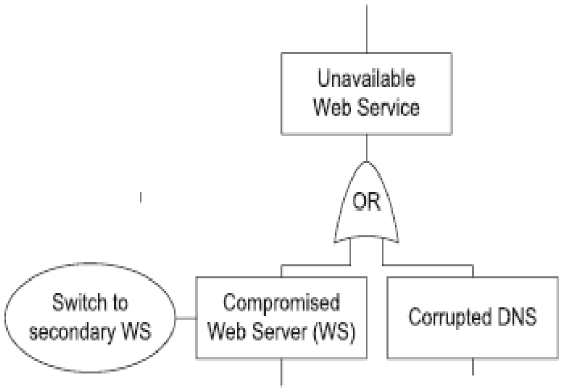


VI. ALGORITHMIC SURVEY TO FINALIZE ALGORITHM

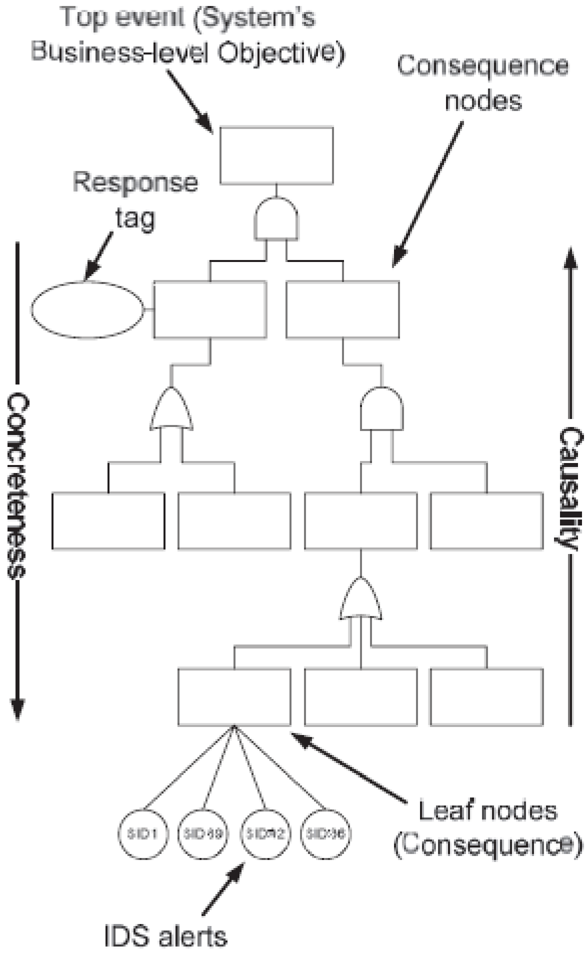
Our engine assigns a game-theoretic response strategy against adversaries sculptural as opponents in a very two-player Stackelberg random game. The RRE applies ART to research unwanted system-level security events among host computers and their countermeasures victimize symbolic logic to combine lower level attack consequences. In addition to, the RRE accounts for uncertainties in intrusion detection alert notifications. The RRE then chooses optimum response actions by determination a partly evident competitive mathematician call method that's automatically derived from attack-response trees. To support network-level multi-objective response choice and contemplate presumably conflicting network security properties, we tend to use symbolic logic theory to calculate the network-level security metric values, i.e., security levels of the system's current and doubtless future states in every stage of the sport.

VII. SURVEY OF THE SELECTED ALGORITHM

Attack Response Tree (ART). To protect a local computing asset, its corresponding local engine first tries to figure out what are the security properties of the asset have been violated as result of an attack, given a received set of alerts. Attack trees offer a convenient way to systematically categorize the different ways in which an asset can be attacked. Local engines make use of a new extended tree (attack) structure, called an attack response tree (ART), that makes it possible 1) to incorporate possible countermeasure (response) actions against attacks, and 2) to consider intrusion detection uncertainties due to false positives and negatives in detecting successful intrusions, while estimating the current security state of the system.



Node Decomposition in ART
Attack Response Tree given below,



VIII. LITERATURE SURVEY TABLE

Paper	Advantages	Disadvantages	Method_Used
Research on Intrusion Detection and Response:A Survey. Year:-July 2005, Author:-Peyman Kabiri and Ali A. Ghorbani	1.Once the detection is reliable, next step would be to protect the network (response). 2. Black Box testing is used for testing the system.	1. Time consuming. 2. Require old data storage for analysis.	1.Honeypot tool a. production honeypot. b. research honeypot 2.Data mining, 3. Bayesian methodology and fuzzy logic approach.
Response Mechanisms for Intrusion Response Systems(IRS) Year:-2009, Author:-N.B. Anuar, S.M.Furnell, M.Papadaki and N.L.Clarke	1. Ability to cooperate with other devices. 2. Using an attack time frame, the relationship between active and passive response.	1. Traditionally may detection Intrusion process. 2. Terminate the network traffic, for current intrusion. 3. Time consuming.	1. Honeypot tool, 2.Using a case-based reasoning method to pre-empt incidents based on historical data
An Implementation of Intrusion Detection System Using Genetic Algorithm. Year:-2012, Author:-Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas	1. Focus on overcoming fidelity, resource usage and reliability problems. 2. Reduces complexity by filtering traffic.	1. Lack of complex equations.	1. Genetic algorithm to efficiently detect various types of network intrusions. 2. KDD99 benchmark dataset: to implement and measure the performance of IDS. 3. Use of standard deviation equations
Intrusion Detection for Smart phone using Cloud Year:-2012, Author:-G.Hemaprabha and Visalatchi.R	1. Smart phone provides “all-in-one” facility. 2. In order to use the services, The smart phones are registered. 3. Wide area connectivity via Internet. 4. It covers large area using cellular networking.	1. A cloud-based service to provide security and tolerance to resource limited mobile phone devices. 2. Large resources are required to give response. 3. Limited free data storage on cloud.	1. The cloud server creates an emulator environment. 2. Cloud computing providers offer their services according to three fundamental models: IaaS, PaaS, and SaaS.
Optimal Game Theory for Network Security Using IPDRS Engine Year:-January 2013, Author:-Shyam Chandran P,Pesmi .A.M	1.Achieves better security 2.Detailed record of intrusion detection reports by IP address	1. Becomes complex for a large network.	1. Client server based approach, a client node sends out a request message to server. The server will receive all details of the client. 4.modules used a. Handling Client: b. Server Responses c. User wardrop Equilibrium: d. Game Theoretic settings: e. Monitoring Client and defending attacker
A Cloud-based Intrusion Detection Forensic Analysis on Smart Phones Year:- April 2013, Author:-I.Raja, P.Sreevenkataramana	1. Indepth analysis is done. 2. Automated response is given by the predefined rules	1. Trust issues with the cloud regarding content of information.	1. Like computer systems even mobile phones are liable to security risk, e.g. viruses, Trojans and worms. 2.Modules: a. Cloud design style b. Client registration & proxy method c. Intrusion detection
Current Studies On Intrusion Detection System, Genetic Algorithm And Fuzzy Logic Year:- March 2013, Author:- Mostaque Md. Morshedur Hassan	1. Misuse detection is IDS analyses the information as gathering and comparing it by large databases of attack signatures. 2. Anomaly detection is to identity deviation by normal behaviors of network traffic and alarm for potential unknown attacks.	1. In anomaly based method there is no clear method for defining normal behavior. 2. In misuse detection slight vaitation in signature cannot be identified. 3. Misuse detection can only detect attacks known to it.	1. Two types of detection a. missuse detection b. anomaly detection 2. Misuse detection system -signature based detection system where well known attacks are represented by signatures. 3. An anomaly-based intrusion detection system inspects ongoing traffic, malicious activities, communication, or behavior for irregularities on networks or systems that could specify an attack.
A Review of Intrusion Detection System in Computer Network Year:- February 2014, Author:-Abhilasha A Sayar, Sunil. N. Pawar and Vrushali Mane	1. IATAC provides the DoD means to secure computer network and communication system. 2. Provide cyber security with wide expansion of LAN and WAN network based Technology.	1. Large data storage is required. 2. Software approach is used to detect intrusion but it is not that much effective. 3. Large hardware is required to develop this IDS.	1. Fuzzy Logic, distinguish data into different labels, as like normal, malicious or any other type. 2. Data mining is used for volume data. 3. Genetic algorithm. 4. Bayesian approach.
Intrusion Detection and Response Using Game Strategy And RRE Engine In Network Security Year:– 2015, Author:-Anuvarsha.G, Rajesh kumar	1. Automation in response to intrusion. 2. Optimum response by consequence nodes for an attack that is detected by IDS. 3. Avoids password remembrance.	1. Detailed architecture not available.	1. An attack-response tree’s (ART) structure is expressed in the node hierarchy, allowing one to decompose an abstract attack goal. 2. The markov decision process (MDP) to find an optimal response. 3. Fuzzy rule set is used (in case of large networks) 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.
Behavior Rule	1. It limits the false	1.Limited Response	1. Analyses a behavior-rule

Specification -based Intrusion Detection for Safety Critical Medical Cyber Physical, systems Author:- Robert Mitchell, Ing-Ray Chen	alarm possibility. 2. Find atmost details of the attack.	mechanism.	specification-based technique 2.Used for intrusion detection of medical devices embedded in a medical cyber physical system (MCPS) 3.It demonstrate the specification based IDS technique can effectively trade higher false positives off for lower false negatives to cope with more sophisticated and hidden attackers.

IX. SYSTEM FEATURE

We provide a high-level architecture of response and recovery engine(RRE), It has two types of decision-making engines at two different layers, i.e., local and global. Moreover, the two layer architecture improves its scalability and performance for large scale computer networks, in which RRE is supposed to protect a large number of Personal computers against malicious attackers. Finally, separation of high-level and low-level security issues significantly simplifies the accurate design of response engines. At the first layer, RRE's local engines are distributed in host computers. Their main inputs consist of intrusion detection system (IDSes) alerts and attack response trees(ART). All IDS alerts are sent to and stored in the alert database to which each local engine subscribes to be notified when any of the alerts related to its host computer is received. The internal architecture of engines includes two components: the state space generator, and the decision engine. Once the inputs has been received, all possible cyber security states, which that the host computer could be in, are generated. These state space might be intractably large; therefore, RRE partially generates the state space generator so that the decision making unit can quickly make decision on the optimal response action. The decision making unit employs a game theoretic algorithm that models attacker RRE interaction as a two player game in which each player tries to maximize his or her benefit. This implies that, once a system is under attack, it is not necessary that immediate greedy response decisions are the best choices, as they may not guarantee the minimum total accumulative cost involved in complete recovery from the attack.

X. CONCLUSION

A game-theoretic intrusion detection and response engine, called the response and recovery engine, was conferred. We modeled the security maintenance of computer networks as a Stackelberg random two-player game during which the attacker and response engine attempt to maximize their own benefits by taking best soul and response actions, respectively. Experiments show that response and recovery engine (RRE) expeditiously takes appropriate step actions against in progress attacks that save system injury and intrusion response value compared to existing static and dynamic government agency solutions.

REFERENCES

[1] Peyman Kabiri and Ali A. Ghorbani, "Research on Intrusion Detection and Response: A Survey" *International Journal of Network Security, Vol.1, No.2, PP.84–102, Sep. 2005 (http://isrc.nchu.edu.tw/ijns/)*

[2] N.B.Anuar, S.M.Furnell, M.Papadaki and N.L.Clarke, "Response Mechanisms for Intrusion Response Systems (IRSs)".

[3] Mohammad Sazzadul Hoque, Md. Abdul Mukit and Md. Abu Naser Bikas, "AN IMPLEMENTATION OF INTRUSION DETECTION SYSTEM USING GENETIC ALGORITHM" *International Journal of Network Security & Its Applications (IJNSA), Vol.4, No.2, March 2012.*

[4] G.Hemaprabha, Visalatchi.R, " Intrusion Detection for Smart phone using Cloud", *International Journal of Computational Engineering Research (IJCER) ISSN: 2250-3005* National Conference on Architecture, Software system and Green computing.

[5] Shyam Chandran P, Resmi .A.M, "Optimal Game Theory for Network Security Using IPDRS Engine", *International Journal of Advanced Research in Computer and Communication Engineering Vol. 4, Issue 1, January 2015.*

[6] I.Raja*, P.Sreevenkataramana," A Cloud-based Intrusion Detection Forensic Analysis on Smart Phones", *Volume 4, No. 4, April 2013 Journal of Global Research in Computer Science.*

[7] Mostaque Md. Morshedur Hassan, "CURRENT STUDIES ON INTRUSION DETECTION SYSTEM, GENETIC ALGORITHM AND FUZZY LOGIC", *International Journal of Distributed and Parallel Systems (IJDPS) Vol.4, No.2, March 2013.*

[8] Abhilasha A Sayar, Sunil. N. Pawar, Vrushali Mane, "A Review of Intrusion Detection System in Computer Network", Abhilasha A Sayar et al, International Journal of Computer Science and Mobile Computing, *Vol.3 Issue.2, February- 2014, pg. 700-703.*

[9] Anuvarsha.G, Rajesh kumar, "Intrusion Detection and Response Using Game Strategy and RRE: Engine In Network Security", International Journal Of Engineering And Computer Science *ISSN:2319-7242 Volume 4 Issue 3 March 2015, Page No. 10977-10983.*

[10] Robert Mitchell, Ing-Ray Chen, "Behavior Rule Specification-based Intrusion Detection for Safety Critical Medical Cyber Physical, systems".

[11] Saman A. Zonouz, Himanshu Khurana, William H. Sanders, Fellow, IEEE, 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.*

Diksha Jadhav, Bachelor of Engineering, Computer Science, Savitribai Phule Pune University, India, Contact number +919422943303

Neha Patil, Bachelor of Engineering, Computer Science, Savitribai Phule Pune University, India, Contact number +919527764179

Parmeshwar Deshmukh, Bachelor of Engineering, Computer Science, Savitribai Phule Pune University, India, Working on RRE: Response and Recovery Engine, Contact number +919552447483

Rohit Patil, Bachelor of Engineering, Computer Science, Savitribai Phule Pune University, India, Contact number +918600869083

Rucha Dixit, Bachelor of Engineering, Professor of Computer Science Department, Savitribai Phule Pune University, India, Contact number +91,