International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

RRE: Network Intrusion Detection System for Response and Recovery Engine.

Diksha Jadhav[1], Neha Patil[2], Parmeshwar Deshmukh[3], Rohit Patil[4], Rucha Dixit[5]

[1]*Bachelor of Engineering, Dept. of computer science, SPPU University, Pune*
[2]*Bachelor of Engineering, Dept. of computer science, SPPU University, Pune*
[3]*Bachelor of Engineering, Dept. of computer science, SPPU University, Pune*
[4]*Bachelor of Engineering, Dept. of computer science, SPPU University, Pune*
[5]*Professor of computer science, Dept. of Computer Engineering, JSPM's JSCOE, Maharashtra, Pune, India*

Abstract - *In the world of fast-spreading attacks requires advance technologies not only in detection algorithms of attacks, but also in automated response techniques to the attacker 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 RRE creates a game-theoretic response strategy against opponents in a two-player Stackelberg stochastic game. The RRE makes use of attack response tree (ART) to analyze undesired system level security events within host computers and their countermeasures. Boolean logic(i.e 0/1) is used to combine lower level attack consequences. The RRE also accounts for the uncertainties in alert notifications(Block or warn) during intrusion detection. The RRE then chooses optimal response (Activate or deactivate)actions after solving a partially observable competitive Markov decision process. It is automatically derived from the 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.*

Key Words: IDS: Intrusion Detection System, ART: Attack Response Tree, RRE: Response and Recovery Engine, Optimal Response strategy, Local and Global Engine

1.INTRODUCTION

The number of intrusions on computer networks are rapidly increasing. This is the reason why preserving the availability and integrity of networked computing systems has turned out to be one of the prime necessity. If we divide the incident handling into three broad classes then First, there are intrusion prevention methods that take actions to prevent occurrence of intrusions, for example, network flow encryption to prevent man-in-the-middle attacks. Secondly, there are intrusion detection systems(IDS), Snort is one of the examples, which try to detect incorrect, inappropriate, or anomalous network activities. These activities could be like, perceiving CrashIIS attacks by detecting malformed packet payloads. Finally, there are 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 intensity of attack damage resulting from delayed response, an automatic i.e non-manual intrusion response is required that provides instantaneous 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 multi-step, sequential, hierarchical, nonzero sum, two-player stochastic game as in where the RRE and the attacker are the two opponents. In each 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. More importantly, ARTs enable RRE to consider inherent uncertainties in alerts received from IDS (i.e., false positive 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 tree into partially observable competitive Markov's 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. It is noteworthy that despite the mathematical cost minimization in RRE that itself requires some time to complete in practice, RRE's ultimate objective is to reduce intrusion response costs and the system damages due to attacks compared to existing intrusion response solutions. This is the game theoretic approach, the RRE adaptively adjusts its behavior according to the attacker's possible 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 granularities, RRE's two-layer architecture consists of local engines, which reside in individual host computers, and the global engine, which resides in the response and recovery server and takes the decision on global response actions once 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 logic rule set. The fuzzy logic rule set is defined using fuzzy numbers, and hence, various input parameters can take on qualitative values such as high or low; therefore, the real-world challenge that accurate specious values of the involved parameters 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 relatively large networks via prototyping and experimentation, demonstrate that it is practical by studying commonly found power grid complicated infrastructure networks. However, we believe that RRE has wide applicability to all kinds of networks.

2. OBJECTIVES

- Preserving the availability and integrity of networked computing systems in the face of fast-spreading intrusions
- Focus is on security problems at intrusion response system.
- Automatic intrusion response System to reduce the damage resulting from delayed response due to Manual Response.

3. ARCHITECTURE

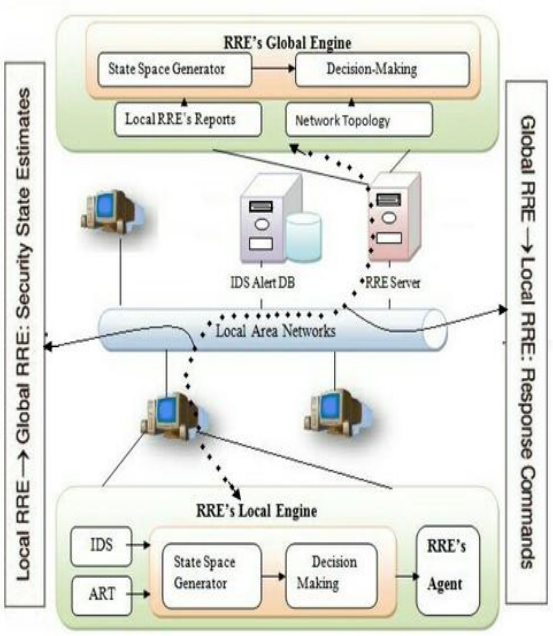
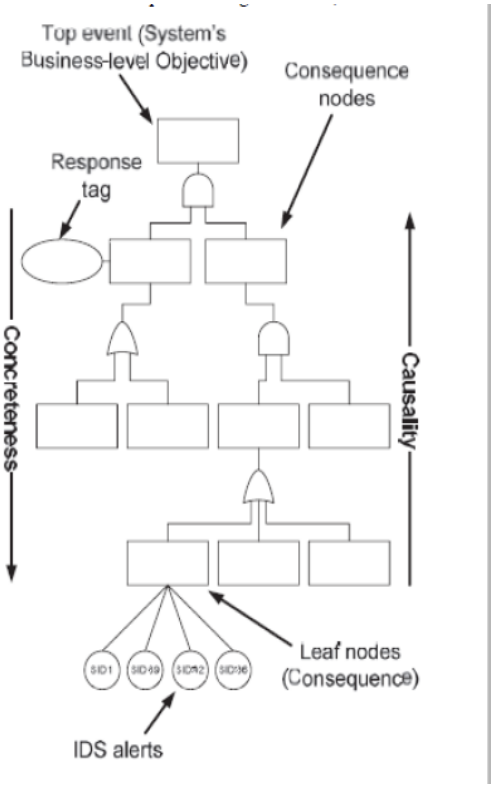


Fig:1 RRE Architecture

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 multi-step, 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.

4. ART

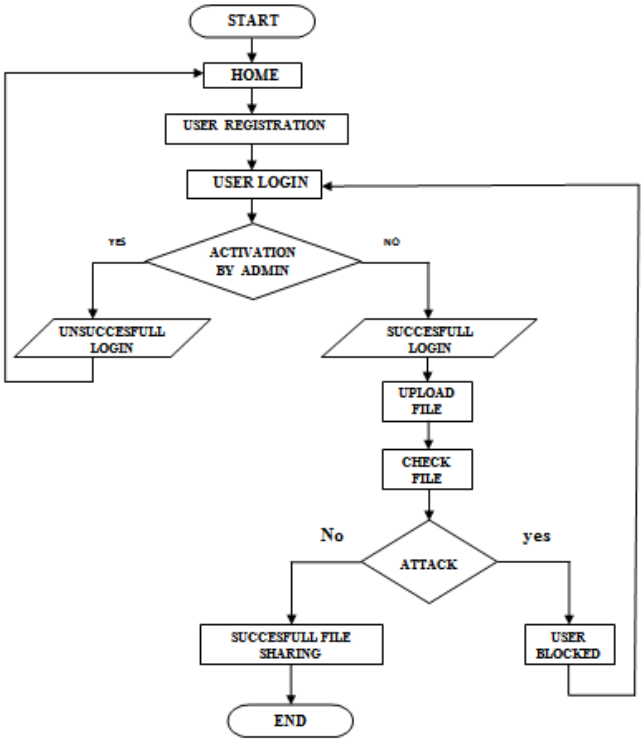


Attack Response Tree (ART). To protect a local computing asset, its corresponding local engine first tries to figure out what are the securities properties of the asset have been violated as result of an attack, given a received set of alerts. Attack trees offer a convenient way to systematically categorize 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.

5. FLOWCHART

It shows sequence of the basic RRE's working,



It checks some conditions and provides access to the systems accordingly.

6. APPLICATION DIAGRAM

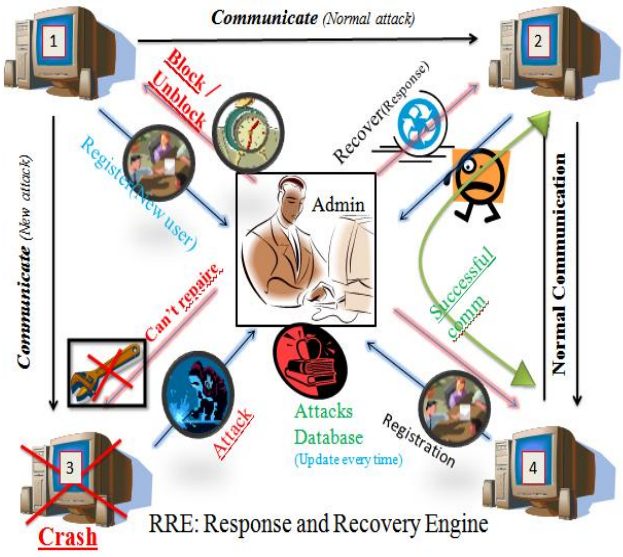


Fig:2 RRE application scenario

There are total three scenarios shown in the fig:2,
All systems must be registered in the network.

1.Normal Communication:

- Node 2 and node 4 shows communication between them via admin i.e. RRE network.

2.Normal Attack:

- Node 1and node 2 shows normal attack scenario, First RRE checks intensity of the attack and give response accordingly(attack must be below 50%).

3.New attack:

- Node 1and node 3 shows new attack scenario, If new attack comes in a network, opponent system will get crash, In between RRE checks victims status and it will block the attacker. Then RRE update its database accordingly.

7.RESULT GRAPH

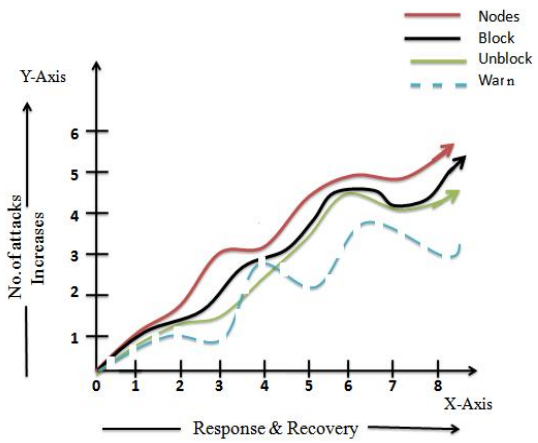


Fig:3 RRE Result graph

Figure 3, shows RRE result graph number of attacks and systems increases in the network(y-axis) with respect to response and recovery(x-axis). Day by day attacks and node are increases, Sometime RRE block or warn to the attacker in the form of response and recover the node (unblock).
Some of them are blocked for specific amount of time or may be lifetime.

8.FUTURE WORK

- RRE can be integrated to be used on a large network with more than 500 nodes.
- RRE can be modified using high quality tools as per the future requirments.
- The concept of RRE can be improvised using precised IDS and well defined ART.

9. CONCLUSIONS

A game-theoretic intrusion detection and response engine, called the response and recovery engine, was conferred. We framework the security maintenance of computer networks as a Stackelberg random two-player game during which the intruder and response engine attempt to maximize their own benefits by taking best soul and response actions, respectively. Experiments show that RRE efficiently takes appropriate countermeasure actions against ongoing attacks that save system damage. The user will be blocked by the admin if the attack is fatal and warning will be given else the file sharing will be successful.

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] 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.*

[3] 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.*

[4] 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.

[5] Diksha Jadhav, Neha Patil, Parmeshwar Deshmukh, Rohit Patil, Rucha Dixit, RRE: Network intrusion detection and Game-Theoretic for response strategy for automated response, International Journal of Engineering and Technical Research (IJETR) ISSN: 2321-0869 (O) 2454-4698 (P), Volume-3, Issue-10, October 2015

[6] 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.

[7] 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.*

[8] 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.*

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

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

BIOGRAPHIES

- Diksha Jadhav,
  Bachelor of Engineering, Computer science, Savitribai Phule Pune University, Working on RRE: Response and Recovery Engine, Contact No. +919422943303.
- Neha Patil,
  Bachelor of Engineering, Computer science, Savitribai Phule Pune University, Working on RRE: Response and Recovery Engine, Contact No. +919527764179.
- Parmeshwar Deshmukh,
  Bachelor of Engineering, Computer science, Savitribai Phule Pune University, Working on RRE: Response and Recovery Engine, Contact No. +919552447483.
- Rohit Patil,
  Bachelor of Engineering, Computer science, Savitribai Phule Pune University, Working on RRE: Response and Recovery Engine, Contact No. +918600869083.
- Rucha Dixit,
  Professor of Computer science, Savitribai Phule Pune University, Working on RRE: Response and Recovery Engine, Contact No. +919623444299.