IJRRECS/May 2015/Volume-3/Issue-5/3897-3901 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

IDENTIFICATION OF INTRUSION EFFORTS BY CONFIRMATION OF ALERTS

D.Naga Kishoreraju[1], U.Sivaji[2]

[1]M.Tech Student, Dept of CSE, St.Martin's Engineering College, Kompally, Hyderabad, T.S, India

[2]Professor, Dept of CSE, St.Martin's Engineering College, Kompally, Hyderabad, T.S, India

ABSTRACT:

For the purpose of reducing severity of attack damage ensuing from delayed response, an automated intrusion reaction is necessary that provides instant response towards intrusion. We suggest a novel approach towards automated response known as response as well as recovery engine that model security conflict between itself and the attacker as a multistep, hierarchical, sequential, two-player stochastic game. Its most important objective is to reduce intrusion response expenses and the system damage because of attacks when compared to existing solutions of intrusion response. Response as well as recovery engine in every step of game, leverages a new wide-ranging attack tree construction known as attack-response tree, and receive alerts for detection of intrusion to assess a variety of security properties of individual host systems within network. Attack-response tree permit response as well as recovery engine to believe intrinsic uncertainties in alerts received from detection of intrusion when estimating system's protection and deciding on response actions. The introduced system is hierarchical organization architecture makes it competent of handling extremely frequent detection of intrusion alerts, and selects most favourable response actions. It contains two kinds of decision-making engines at two distinct layers that are local as well as global.

Keywords: Attacker, Response as well as recovery engine, Intrusion detection, Hierarchical structure, Security.

1. INTRODUCTION:

For prevention as well as detection of intrusion, for the most part of research were focused on getting better techniques.

While intrusion response remains a manual procedure performed by network administrators certainly introduces some delay among notification and response, which might be easily exploited by attacker to significantly enhance the damage. In our work we put forward a new approach towards automated response known as response as well as recovery engine (RRE). It models security battle among itself and the attacker as a multistep, hierarchical, sequential, stochastic game concerning two players. In each move, response as well as recovery engine leverages a new comprehensive attack tree construction known as attack-response tree (ART), and receive alerts for detection of intrusion to assess a variety of security properties of individual host systems within network[1]. Attack-response tree offer a recognized way to explain host system security on basis of likely intrusion and response situation for attacker and response engine. By means of game theoretic approach, proposed engine adjusts its behaviour consistent with attacker's promising future reactions, consequently preventing attacker from causing important damage towards system by taking an efficiently selected sequence of actions. To handle security issues with several granularities, response as well as recovery engine two-layer construction includes local engines, which exist in individual host computers, as well as global engine, which exist in response as well as recovery server and choose global response activities once the system, is not recovered by local engines. Hierarchical building of projected system makes it competent of handling extremely frequent detection of intrusion alerts, and selects most favourable response actions and it gets better scalability, performance of response as well as recovery engine, with the intention that it can defend computing assets against attackers in important computer networks.

2. METHODOLOGY:

For dropping severity of attack damage ensuing from postponed response, an automatic intrusion reaction is necessary that provides instant response towards intrusion. Our engine utilizes a game-theoretic response scheme against adversaries modelled as opponents within stochastic game of two players. It apply

attack-response trees towards analyzing unwanted system-level protection events within host computers that put forward a standard method to make clear host system security on basis of likely intrusion and response situation for attacker and response engine. The proposed system accounts for doubts in notifications of intrusion detection alerts [2]. Attack-response tree allow response as well as recovery engine to believe intrinsic uncertainties in alerts received from detection of intrusion when estimating system's protection and deciding on response actions. By game theoretic approach, projected engine regulates its behaviour in agreement with attacker's promising future reactions, consequently preventing attacker from causing important damage towards system by taking an efficiently selected sequence of actions. Regardless of mathematical cost minimization in response as well as recovery engine that itself need some time to complete. Actually, response as well as recovery engine eventual objective is to reduce intrusion response expenses and the system damage because of attacks when compared to existing solutions of intrusion response [3][4]. To support network-level intrusion reaction where comprehensive security level is often function of altered particular properties, response as well as recovery engine utilizes a fuzzy control-based method that can take into explanation quite a few objective functions concurrently.

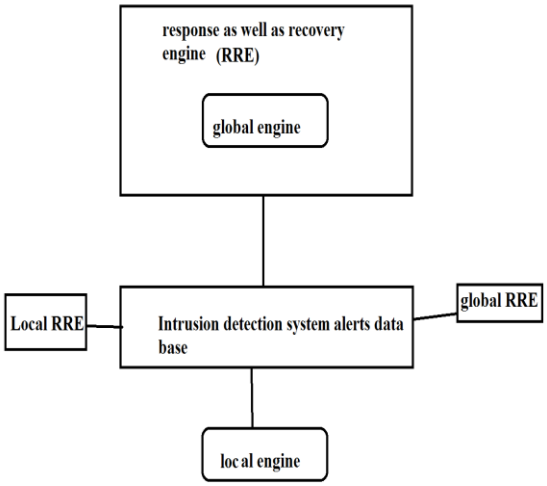

Fig1: An overview of introduced system.

3. DESIGNING OF RESPONSE AS WELL AS RECOVERY ENGINE:

An approach was introduced in our work towards automated response known as response as well as recovery engine. To hold security issues with quite a lot of granularities, response as well as recovery engine two-layer construction consists local engines, existing in individual host computers, as well as global engine, which exist in response as well as recovery server and choose global response activities once the system, is not recovered by local engines. Its critical objective is to reduce

intrusion response expenses and the system damage because of attacks when compared to existing solutions of intrusion response. It has two kinds of decision-making engines at two distinct layers that are local as well as global as shown in fig1. This hierarchical organization of proposed system architecture makes it competent of handling extremely frequent detection of intrusion alerts, and selects most favourable response actions. The two layer building improves its scalability for important computer networks, in which response as well as recovery engine is supposed to defend a huge number of host computers against malevolent attackers. Separation of high as well as low-level security issues considerably simplifies accurate designing of response engines. At the initial layer, response as well as recovery engine local engines are dispersed in host computers and their most important inputs consist of detection of intrusion alerts and attack-response trees [5]. The entire detection of intrusion alerts are stored in alert database to which every local engines subscribes to be informed when any of alerts connected to its host computer is obtained. The internal structural design of engines includes two most important components such as state space generator, as well as decision engine. Proposed response as well as recovery engine global engine, as its second layer, gets hold of high-level information from the entire host computers within the network, make a decision on best possible global response actions to get, and coordinate response as well as recovery engine agents to achieve actions by means of sending them appropriate response commands. Additionally to local security estimates from host computers, network topology in addition to global network access control policies are moreover fed into global engine. Response as well as recovery engine converts network topology as well as access control policies into competitive Markov decision process representation automatically. Response as well as recovery engine employs described network-level security properties like security metrics to choose the most favourable network level response action by means of solving generated network model [6].

4. CONCLUSION:

A new approach was introduced in our work towards automated response known as response as well as recovery engine. It models protection issues among itself and the attacker as a multistep, hierarchical,

sequential, two-player stochastic game, The system adjusts its performance consistent with attacker's promising future reactions, consequently preventing attacker from causing important damage towards system by taking an efficiently selected sequence of actions. Response as well as recovery engine in each step of game, leverages a new comprehensive attack tree construction known as attack-response tree, and receive alerts for detection of intrusion to assess a variety of security properties of individual host systems within network. Attack-response tree suggest a predictable means to explain host system security on basis of likely intrusion and response situation. The introduced system objective is to reduce intrusion response expenses and the system damage because of attacks when compared to existing solutions of intrusion response. Hierarchical proposal gets better scalability, performance of response as well as recovery engine, with the intention that it can defend computing assets against attackers in important computer networks. For managing network-level intrusion reaction response as well as recovery engine utilizes a fuzzy control-based method that can take into explanation quite a few objective functions simultaneously.

REFERENCES

[1] 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.

[2] 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.

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

[4] 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, pp. 2344-2349, 2000.

[5] O.P. Kreidl and T.M. Frazier, "Feedback Control Applied to Survivability: A Host-Based Autonomic Defense System," IEEE Trans. Reliability, vol. 53, no. 1, pp. 148-166, Mar. 2004.

[6] 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.