IJRRECS/June 2015/Volume-3/Issue-6/4230-4234 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EXPOSURE TOWARDS RECOGNISING INTRUSION ATTEMPTS IN NETWORK SYSTEMS

K.Srinivas[1], Dr.K.Srujan Raju[2]

[1]M.Tech Student, Dept of CSE, CMR Technical Campus, Hyderabad, T.S, India

[2]Professor & HOD, Dept of CSE, CMR Technical Campus, Hyderabad, T.S, India

ABSTRACT:

For the most of efforts were made on improvisation for intrusion prevention as well as detection. To reduce the severity of attack damage that is resulting from postponed response, an automated intrusion reaction is mandatory that provides instantaneous response towards intrusion. We introduce an automated cost-sensitive intrusion response system known as response and recovery engine that model security battle among itself and attacker as hierarchical and sequential two-player stochastic game. The proposed system usually converts attack response trees into partly noticeable competitive Markov decision procedure that are solved to discover the most favourable response action against attacker. Attack-response tree put forward a recognized means to explain host system security on basis of promising intrusion and response scenarios for attacker and response engine, respectively. The system of response and recovery engine ultimate objective is to save the costs of intrusion response and system damages because of attacks that are compared to traditional solutions of intrusion response. It is computationally practical for comparatively large networks by means of prototyping.

Keywords: Response and recovery engine, Markov decision, Attack-response tree, Attacker, Intrusion prevention.

1. INTRODUCTION:

Estimation of intrusion detection systems alerts as well as managing of response efforts is moreover capable to communicate with their peers at different network layers [1]. There are techniques of intrusion response that take reactive actions on the basis of received alerts of intrusion detection systems to stop attacks prior to significant damage and to make sure protection of computing environment. Intrusion response typically remains a manual procedure that is performed by network administrators who are informed by intrusion detection systems alerts and act in response to intrusions. This manual response procedure certainly commences some delay among notification as well as response, which might be effortlessly exploited by attacker to attain their goal and considerably enhance the damage. To lessen the severity of attack damage that is resulting from postponed response, an automated intrusion reaction is mandatory that provides instant response to intrusion. we put forward an automated cost-sensitive intrusion response system known as response and recovery engine (RRE) that model security battle among itself and attacker as a multistep, hierarchical, sequential two-player stochastic game. Our engine utilizes a game-theoretic response scheme against adversaries modelled as opponents within a two-player Stackel berg stochastic game [2][3]. The response and recovery engine applies attack-response trees to analyze undesirable system-level security actions within host computers to merge lower level attack consequences. To handle with protection issues with several granularities, response and recovery engine two-layer structural design as shown in fig1 consists of local engines, which reside in particular host computers, and global engine, which resides in response and recovery server and come to a decision on global response activities once the system is not recovered by local engines. To manage network-level intrusion response in which global security level is often a function of various specific properties, Response and recovery engine employs a fuzzy control-based method that can consider quite a lot of objective functions concurrently.

2. METHODOLOGY OF RESPONSE AND RECOVERY ENGINE:

In each step of game, response and recovery engine leverages a novel extended attack tree structure, known as attack-response tree, and received intrusion detection

systems alerts to assess a variety of security properties of individual host systems within network. Attack-response tree enable response and recovery engine to consider intrinsic uncertainties in alerts that are received from intrusion detection systems when estimating system's security as well as making a decision on response actions. Attack-response tree present a recognized means to explain host system security on basis of promising intrusion and response scenarios for attacker and response engine, correspondingly. Response and recovery engine usually converts attack response trees into partly noticeable competitive Markov decision procedure that are solved to discover the most favourable response action against attacker, in sense that utmost low-priced accumulative damage that attacker can cause in game is reduced. Response and recovery engine achieves the objectives with a unified modelling approach where game theory as well as Markov decision processes are combined. It is remarkable that regardless of the mathematical cost minimization in Response and recovery engine that it necessitates some time to complete [4]. In fact, response and recovery engine ultimate intention is to save the costs of intrusion response and system damages because of attacks that are compared to traditional solutions of intrusion response. Our engine utilizes a game-theoretic response scheme against adversaries modelled as opponents within a two-player Stackel berg stochastic game. Using game theoretic approach, response and recovery engine adaptively alter its actions in relation to attacker's promising future reactions, hence preventing attacker from causing considerable damage to system by means of an intelligently selected sequence of actions. Response and recovery engine is computationally resourceful for comparatively large networks by means of prototyping. It was considered as practical by means of studying generally found power grid important infrastructure networks.

3. IMPROVISATION OF INTRUSION RESPONSE:

Response and recovery engine extends state of the art within intrusion response in three basic ways. Initially response and recovery engine accounts for considered adversarial actions in which attacks take place in stages where adversaries carry out well-planned schemes and deal with defence measures that are taken by system administrators all along the way. It does so by means of

applying game theory and looking for responses that optimize on long-standing gains. Response and recovery engine simultaneously accounts for intrinsic uncertainties in intrusion detection systems alert notifications by attack-response trees converted to a partially apparent Markov decision process that work out optimal responses in spite of these uncertainties. This is significant since intrusion detection systems these days and in near future will be not capable to produce alerts that match completely towards effective intrusions, and response techniques have to permit for this imperfection to be practical. For ease of design rationale, response and recovery engine permit network security administrators to describe properties of high-level network security all the way through easy to follow linguistic terms for particular target network [5]. This is a critical provision that response and recovery engine provides, since contrasting system-level security properties, for instance, web server accessibility, which is reused across networks, the properties of network-level security typically have to be defined particularly for each network by security administrators. Response and recovery engine achieves the goals with a unified modelling approach where game theory as well as Markov decision processes are combined. Hierarchical architecture gets better scalability, ease of design, as well as performance of response and recovery engine, with the intention that it can defend computing assets against attackers in extensive computer networks. To administer network-level intrusion response in which global security level is often a function of various specific properties, Response and recovery engine employs a fuzzy control-based method that can consider quite a lot of objective functions concurrently. The fuzzy rule set is described by means of fuzzy numbers, and therefore, a variety of input parameters can make use of qualitative values therefore, real-world challenge that precise crisp values of concerned parameters are not constantly recognized is addressed totally. Especially, reports from local engines are fed into global response engine fuzzy system. Then, response and recovery engine computes quantitative scores of promising network-level response activities by means of its earlier defined fuzzy rule set [6].

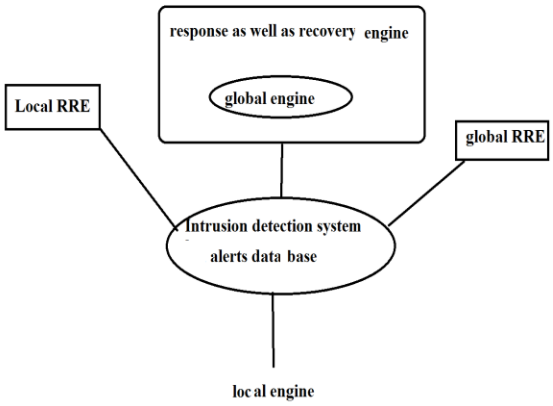

Fig1: An overview of proposed system.

4. CONCLUSION:

Intrusion response usually remains a manual process that is performed by network administrators who are informed by intrusion detection systems alerts and act in response to intrusions. we introduce cost-sensitive intrusion response system recognized as response and recovery engine that model security battle among itself and attacker as a multistep, hierarchical, sequential two-player stochastic game. The system applies attack-response trees to analyze undesirable system-level security actions within host computers to merge lower level attack consequences. It typically converts attack response trees into partly noticeable competitive Markov decision procedure that are solved to discover the most favourable response action against attacker. Response and recovery engine is computationally capable for comparatively large networks by means of prototyping. The proposed system intention is to save the costs of intrusion response and system damages because of attacks that are compared to traditional solutions of intrusion response. Attack-response tree put forward a recognized means to explain host system security on basis of promising intrusion and response situations for attacker and response engine respectively.

REFERENCES

[1] 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.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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