IJRRECS/November 2015/Volume-3/Issue-11/4924-4929 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

AN EFFECTIVE AUTOMATED SCHEME FOR OFFERING RESPONSE TO INTRUSION

G.Tejaswi[1], A.Nalini[2], B.M.Rao[3]

[1]**M.Tech Student, Dept of CSE, Malineni Lakshmaiah Women's Engineering College, Guntur, A.P, India**

[2]**Assistant Professor, Dept of CSE, Malineni Lakshmaiah Women's Engineering College, Guntur, A.P, India**

[3]**Associate Professor& HOD, Dept of CSE, Malineni Lakshmaiah Women's Engineering College, Guntur, A.P, India**

ABSTRACT:

There are methods of intrusion response that get responsive actions on basis of received alerts of Intrusion detection system to prevent attacks earlier than causing important damage and to make sure computing environment security. For decreasing damage severity that results from delayed response, automated intrusion response is necessary that offer immediate response towards intrusion. We suggest an automated response known as response and recovery engine which will utilize game-theoretic response approach against adversaries modelled in two-player stochastic game. It will support multi-objective response selection of network-level and imagine contradictory security properties of network. Proposed system engine will apply attack-response trees to estimate unwanted security events of system-level in host computers by means of Boolean logic to merge lower level attack effects. Attack-response trees explain host system security on basis of intrusion and response situations for attacker. For managing of network-level intrusion response in which global security level is moreover a function of various particular properties, response and recovery engine will employs a fuzzy control-based method that can consider various objective functions at the same time. Fuzzy logic theory was used to work out network-level security metric in each stage of game.

Keywords: Intrusion detection system, Response and recovery engine, Attack-response trees, Fuzzy logic theory, Automated intrusion response, Game-theory.

1. INTRODUCTION:

Most of research has spotlighted on methods of improvisation for detection of intrusion, whereas intrusion response remains manual procedure that is carried out by network administrators who will respond to intrusions [1]. This process will unavoidably set up some delay among notification as well as response, which might be exploited by attacker who appreciably increases the damage. For reducing severity of damage that results from delayed response, automated intrusion response is necessary that offer immediate response towards intrusion. In our work we propose an automated response known as response and recovery engine which will utilize game-theoretic response approach against adversaries modelled in two-player Stackelberg stochastic game. Response and recovery engine will account for uncertainties in notifications of intrusion detection alert. onse and recovery engine will select the actions of best possible response by means of solving partially visible competitive Markov decision procedure that is derived from attack-response trees [2][3]. Response and recovery engine will apply attack-response trees to estimate unwanted security events of system-level in host computers by means of Boolean logic to merge lower level attack effects. The proposed system will support multi-objective response selection of network-level and imagine contradictory security properties of network. We make use of fuzzy logic theory to compute network-level security metric in each stage of game. Particularly inputs towards game-theoretic response selection engine of network level are fed into fuzzy structure that is responsible of nonlinear inference as well as quantitative ranking of actions by means of its earlier defined fuzzy rule set. Finally best possible actions of network-level response are selected all the way through a game-theoretic optimization procedure.

2. METHODOLOGY:

Preservation of reliability of networked computing systems regardless of fast-spreading intrusions needs advances in detection algorithms and also in automated response techniques. There are methods of intrusion prevention that prevent occurrence of attacks. There are systems of intrusion detection which notice improper, or else inconsistent network activities. We suggest an automated response known as response

and recovery engine which will utilize game-theoretic response approach against adversaries modelled in two-player Stackelberg stochastic game. In every game step, response and recovery engine will control a novel extended attack tree arrangement, known as attack-response tree and received detection of intrusion alerts to assess a variety of security properties of individual host systems within network. Response and recovery engine will apply attack-response trees to estimate unwanted security events of system-level in host computers by means of Boolean logic to merge lower level attack effects. Attack-response trees will present formal method to explain host system security on basis of intrusion and response situations for attacker. Attack-response trees will permit response and recovery engine to consider intrinsic uncertainties in alerts that are received from intrusion detection systems during estimation of system security. The proposed engine will account for uncertainties in notifications of intrusion detection alert. onse and recovery engine will select the actions of best possible response by means of solving partially visible competitive Markov decision procedure that is derived from attack-response trees [4]. The proposed scheme will support multi-objective response selection of network-level and imagine contradictory security properties of network. It will extend state of the art in intrusion response in three basic methods. Response and recovery engine will account for considered adversarial behaviour where attacks take place in stages where adversaries will implement well-planned scheme. It does by application of game theory and looking for responses that optimize on continuing gains. Secondly, Response and recovery engine accounts for intrinsic uncertainties in intrusion detection systems alert notifications by attack-response trees that are converted to partly visible Markov decision process that work out best possible responses in spite of these uncertainties. Since intrusion detection systems will be incapable to produce alerts that match up promising intrusions, and response techniques have to, thus permit for this limitation to be practical [5]. Thirdly, for easiness of design intention, response and recovery engine permit security administrators to describe security properties of high-level network and this is an essential facility that response and recovery engine provides, because of different system-level

security properties [6]. Response and recovery engine will attain above three goals by means of a combined modelling technique where game theory and Markov decision procedures are combined.

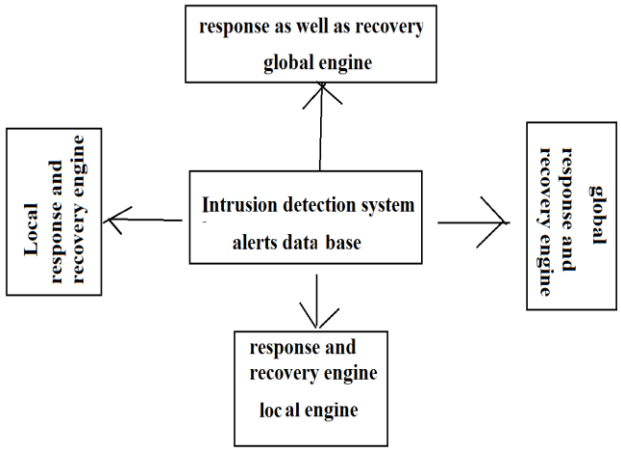

Fig1: Proposed system.

3. AN OVERVIEW OF PROPOSED SYSTEM:

For dropping severity of damage that results from delayed response, automated intrusion response is necessary that offer immediate response towards intrusion. We propose an automated response known as response and recovery engine which will utilize game-theoretic response approach against adversaries. For managing with security issues with dissimilar granularities, response and recovery engine will use two-layer architecture that includes of local engines, which exist in individual host computers, and global engine, which exist in response as well as recovery server and make a decision on actions of global response when system is not recovered by local engines. Hierarchical structural design will improve scalability as well as performance of response and recovery engine, so that it can defend computing resources against attackers. Response and recovery engine will control a novel extended attack tree arrangement, known as attack-response tree and received detection of intrusion alerts to assess a variety of security properties of individual host systems within network. Attack-response trees will authorize response and recovery engine to consider intrinsic uncertainties in alerts that are received from intrusion detection systems during estimation of system security. For supporting network-level intrusion response in which global security level is moreover a function of various particular properties, response and recovery engine will employs a fuzzy control-based method that can consider various objective functions at the same time. Fuzzy logic theory was used to compute network-level security metric in each stage of game. Inputs in the direction of game-theoretic response selection engine of network level are fed into fuzzy structure

that is responsible of nonlinear inference as well as quantitative ranking of actions by means of its earlier defined fuzzy rule set. At last best possible actions of network-level response are selected all the way through a game-theoretic optimization procedure.

4. CONCLUSION AND FUTURE WORK:

Consistency protection of networked computing systems regardless of fast-spreading intrusions needs advancement in detection algorithms and also in methods of automated response. Severity of intrusions on computer networks is quickly increasing. For reduction of severity of damage that results from delayed response, automated intrusion response is necessary that offer immediate response towards intrusion. We propose response and recovery engine which will utilize game-theoretic response approach against adversaries modelled in two-player stochastic game. Response and recovery engine accounts for uncertainties in notifications of intrusion detection alert and will apply attack-response trees to estimate unwanted security events of system-level in host computers. Proposed scheme will support multi-objective response selection of network-level and imagine contradictory security properties of network. Fuzzy logic theory was used to compute network-level security metric in each stage of game. Finest possible actions of network-level response are selected all the way through a game-theoretic optimization procedure.

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 due to their reliance on local responses and specific profile based IDS. Game theory in an IRS-related context has also been utilized in previous papers. 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. 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 action.

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] E. LeMay, M.D. Ford, K. Keefe, W.H. Sanders, and C. Muehrcke, "Model-Based Security Metrics Using Adversary View Security Evaluation (Advise)," Proc. Int'l Conf. Quantitative Evaluation of Systems (QEST), pp. 191-200, 2011.

[5] R.C. Berkan and S. Trubatch, Fuzzy System Design Principles, first ed. Wiley-IEEE Press, 1997.

[6] S.-J. Chen and S.-M. Chen, "Fuzzy Risk Analysis Based on Similarity Measures of Generalized Fuzzy Numbers," IEEE Trans. Fuzzy Systems, vol. 11, no. 1, pp. 45-56, Feb. 2003.