ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Protecting Integrity of Networks using a Game-Theoretic Intrusion Response and Recovery Engine

Kedasi Srinivas
M.Tech Student
Department of CSE,
St.Peter's Engineering College,
Hyderabad, TS, INDIA

Mr. Anjaiah Adepu
Assistant Professor
Department of CSE,
St.Peter's Engineering College,
Hyderabad, TS, INDIA

M.Mounika
Assistant Professor
Department of CSE,
St.Peter's Engineering College,
Hyderabad, TS, INDIA

Abstract:

With the increasing number of network technology, intruders are also rationally increased. To provide the security to the network from the intruders is one of the vital one, this survey presents Intrusion Response System to handle the intruders by request and response process by using Game theory. This survey provides a better understanding of the different research approaches by applying game theory for the Automated Intrusion Response System (AIRS). Preserving the availability and integrity of networked computing systems in the face of fast-spreading intrusions requires advances not only in detection algorithms, but also in automated response techniques. In this paper, we propose a new approach to automated response called the response and recovery engine (RRE). Our engine employs a game-theoretic response strategy against adversaries modeled as opponents in a two-player Stackelberg stochastic game. The RRE applies attack-response trees (ART) to analyze undesired system-level security events within host computers and their countermeasures using Boolean logic to combine lower level attack consequences. In addition, the RRE accounts for uncertainties in intrusion detection alert notifications. The RRE then chooses optimal response actions by solving a partially observable competitive Markov decision process that is automatically derived from attack-response trees. To support network-level multiobjective response selection and consider possibly conflicting network security properties, we employ fuzzy logic theory to calculate the network-level security metric values, i.e., security levels of the system's current and potentially future states in each stage of the game. In particular, inputs to the network-level game-theoretic response selection engine are first fed into the fuzzy system that is in charge of a nonlinear inference and quantitative ranking of the possible actions using its previously defined fuzzy rule set. Consequently, the optimal network-level response actions are chosen through a game-theoretic optimization process. Experimental results show that the RRE, using Snort's alerts, can protect large networks for which attack-response trees have more than 500 nodes.

Introduction

The severity and number of intrusions on computer networks are rapidly increasing. Generally, incident-handling [9] techniques are categorized into three broad classes. First, there are intrusion prevention methods that take actions to prevent occurrence of attacks, e.g., network flow encryption to prevent man-in-the-middle attacks. Second, there are intrusion detection systems (IDSes), such as Snort [22], which try to detect inappropriate, incorrect, or anomalous network activities, e.g., perceiving CrashIIS attacks by detecting malformed packet payloads. Finally, there are intrusion response techniques that take responsive actions based on received IDS alerts to stop attacks before they can cause significant damage and to ensure safety of the computing environment. So far, most research has focused on improving techniques for intrusion prevention and detection, while intrusion response usually remains a manual process performed by network administrators who are notified by IDS alerts and respond to the intrusions. This manual response process inevitably introduces some delay

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

between notification and response, which could be easily exploited by the attacker to achieve his or her goal and significantly increase the damage [6]. Therefore, to minimize the severity of attack damage resulting from delayed response, an automated intrusion response is required that provides instantaneous response to intrusion. During the last five years, three types of techniques aimed at enhancing automation in the intrusion response were proposed. The majority of those techniques are based on lookup tables filled with predefined mappings, e.g., (response actions, intrusion alerts) [24]. These methods allow response systems to deal with intrusions faster. However, they suffer from a lack of 1) flexibility, mainly because these systems completely ignore the intrusion cost factor; and 2) scalability, since it is infeasible to predict all the alert combinations from IDSes in a large-scale computer network. A second group of intrusion response systems (IRSes) employs a dynamic rule-based selection procedure [28] that selects response actions based on a certain attack metric, e.g., confidence or severity of attack. Finally, there has been increasing interest in developing cost-sensitive models of response selection [26]. The main objective in applying such a model is to compare intrusion damage and response cost to ensure system recovery with minimum cost without sacrificing the normal functionality of the system under attack.

In this paper, we present an automated cost-sensitive intrusion response system called the Response and Recovery Engine (RRE) that models the security battle between itself and the attacker as a multi-step, sequential, hierarchical, non-zero-sum, two-player stochastic game. In each step of the game, RRE leverages a new extended attack tree structure, called the attack-response tree (ART), and the received IDS alerts to evaluate various security properties of the system. ARTs provide a formal way to describe 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 IDSes (i.e., false positive and false negative rates) when estimating the system's security and deciding on response actions. Then, the RRE automatically converts the attack-response trees into partially observable competitive Markov 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. Using this game-theoretic approach, RRE adaptively adjusts its behavior according to the attacker's possible future reactions, thus preventing 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 decides on global response actions once the system, is not recoverable by the local engines. Furthermore, the hierarchical architecture improves scalability, ease of design, and performance of RRE, so that it can protect computing assets against attackers in large-scale computer networks.

The contributions of RRE are as follows. First, RRE accounts for planned adversarial behavior in which attacks occur in stages in which adversaries execute well-planned strategies and address defense measures taken by system administrators along the way. It does so by applying game theory and seeking responses that optimize on long-term gains. Second, RRE concurrently accounts for inherent uncertainties in IDS alert notifications with attack-response trees converted to partially observable Markov decision processes that compute optimal responses despite these uncertainties. This is important because IDSes today and in the near future will be unable to generate alerts that match perfectly to successful intrusions, and response techniques must therefore allow for this imperfection in order to be practical. RRE achieves the above two goals with a unified modeling approach in which game theory and Markov decision processes are combined.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We demonstrate that RRE is computationally efficient for relatively large networks via prototyping and experimentation, and demonstrate that it is practical by studying commonly found critical infrastructure networks associated with the power grid. However, we believe that RRE has wide applicability to all kinds of networks.

EXISTING SYSTEM:

The severity and number of intrusions on computer networks are rapidly increasing. Generally, incident-handling techniques are categorized into three broad classes. First, there are intrusion prevention methods that take actions to prevent occurrence of attacks, for example, network flow encryption to prevent man-in-the-middle attacks.

Second, there are intrusion detection systems (IDSes), such as Snort, which try to detect inappropriate, incorrect, or anomalous network activities, for example, perceiving CrashIIS attacks by detecting malformed packet payloads. Finally, there are intrusion response techniques that take responsive actions based on received IDS alerts to stop attacks before they can cause significant damage and to ensure safety of the computing environment. So far, most research has focused on improving techniques for intrusion prevention and detection, while intrusion response usually remains a manual process performed by network administrators who are notified by IDS alerts and respond to the intrusions. This manual response process inevitably introduces some delay between notification and response.

DISADVANTAGES OF EXISTING SYSTEM:

- Which could be easily exploited by the attacker to achieve his or her goal and significantly increase the damage.

- To reduce the severity of attack damage resulting from delayed response, an automated intrusion response is required that provides instantaneous response to intrusion.

PROPOSED SYSTEM:

In this paper, we present an automated cost-sensitive intrusion response system called the response and recovery engine (RRE) that models the security battle between itself and the attacker as a multistep, sequential, hierarchical, non zero sum, two-player stochastic game. In each step of the game, RRE leverages a new extended attack tree structure, called the attack-response tree (ART), and received IDS alerts to evaluate various security properties of the individual host systems within the network.

ARTs provide 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 IDSes (i.e., false positive and false negative rates), when estimating the system's security and deciding on response actions.

Then, the RRE automatically converts the attack-response trees into partially observable competitive Markov 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.

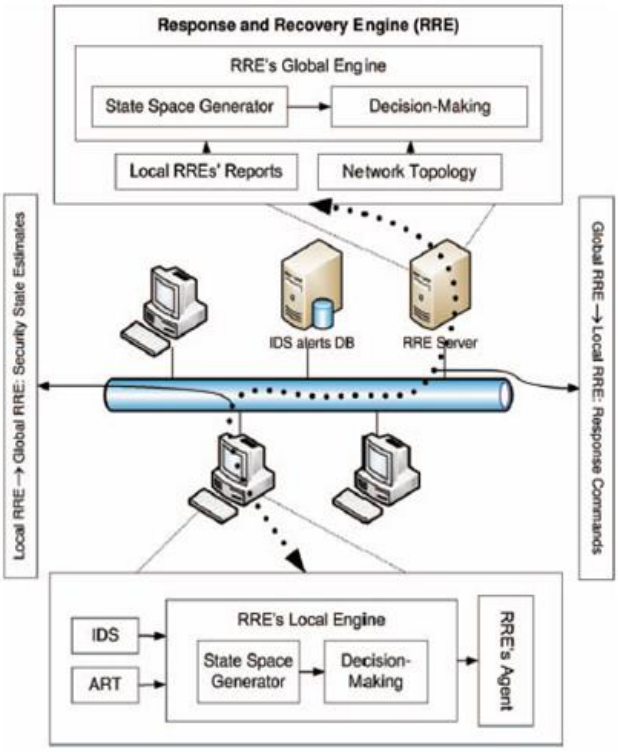
ADVANTAGES OF PROPOSED SYSTEM:

- Improves its scalability for large-scale computer networks, in which RRE is supposed to protect a large number of host computers against malicious attackers.

- Finally, separation of high- and low-level security issues significantly simplifies the accurate design of response engines.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SYSTEM ARCHITECTURE:



Conclusion

A game-theoretic intrusion response engine, called the Response and Recovery Engine (RRE), was presented. We modeled the security maintenance of computer networks as a Stackelberg stochastic two-player game in which the attacker and response engine try to maximize their own benefits by taking optimal adversary and response actions, respectively. Using an extended attack tree structure called the Attack-Response Tree (ART), RRE explicitly takes into account inaccuracies associated with IDS alerts in estimating the security state of the system. Moreover, RRE explores the intentional malicious attacker's next possible action space before deciding upon the optimal response action, so that it is guaranteed that the attacker cannot cause greater damage than what RRE predicts. Experiments show that RRE takes appropriate countermeasure actions against ongoing attacks, and brings an insecure network to its normal operational mode with the minimum possible cost.

References

[1] Saman A. Zonouz, Himanshu Khurana, William H. Sanders, 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.

[2] A. Avizienis, J. Laprie, B. Randell, and C. Landwehr. Basic concepts and taxonomy of dependable and secure computing. IEEE Trans. on Dep. and Sec. Comp., 1:11–33, 2004.

[3] I. Balepin, S. Maltsev, J. Rowe, and K. Levitt. Using specification-based intrusion detection for automated response. Proc. of the Int'l Symp. on Recent Advances in Intrusion Detection, pages 136–54, 2003.

[4] R. Bellman. Dynamic Programming. Princeton University Press, 1957; republished 2003.

[5] M. Bloem, T. Alpcan, and T. Basar. Intrusion response as a resource allocation problem. Proc. of Conf. on Decision and Control, pages 6283–8, 2006.

[6] A. Cassandra. Exact and Approximate Algorithms for Partially Observable Markov Decision Processes. PhD thesis: Brown University, 1998.

[7] F. Cohen. Simulating cyber attacks, defenses, and consequences. Journal of Comp. and Sec., 18:479–518, 1999.

[8] T. Dean, L. Kaelbling, J. Kirman, and A. Nicholson. Planning under time constraints in stochastic domains. Artificial Intelligence, 76:35–74, 1995.

[9] J. Filar and K. Vrieze. Competitive Markov Decision Processes. Springer-Verlag, 1997.

[10] B. Foo, M. Glause, G. Howard, Y. Wu, S. Bagchi, and E. Spafford. Information assurance: Dependability and Security in Networked Systems. Morgan Kaufmann, 2007.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[11] B. Foo, Y. Wu, Y. Mao, S. Bagchi, and E. Spafford. Adepts: adaptive intrusion response using attack graphs in an ecommerce environment. Proc. of Dependable Systems and Networks, pages 508–17, 2005.

[12] S. Hsu and A. Arapostathis. Competitive Markov decision processes with partial observation. Proc. of IEEE lnt. Conf. on Systems, Man and Cybemetics, 1:236–41, 2004.

[13] L. Kaelbling, M. Littman, and A. Cassandra. Partially observable Markov decision processes for artificial intelligence. Proc. of the German Conference on Artificial Intelligence: Advances in Artificial Intelligence, 981:1–17, 1995.

[14] O. P. Kreidl and T. M. Frazier. Feedback control applied to survivability: A host-based autonomic defense system. IEEE Trans. on Reliability, 53:148–66, 2004.

[15] C. Kruegel, W. Robertson, and G. Vigna. Using alert veri- fication to identify successful intrusion attempts. Info. Processing and Communication, 27:220–8, 2004.