International Research Journal of Innovations in Engineering and Technology (IRJIET)

ISSN (online): 2581-3048

Volume 3, Issue 7, pp 46-48, July-2019

An Automated Response and Recovery Engine (RRE): Responses against Intrusion

M Nayak Hanumanthu

Assistant Professor, Department of Computer Science And Engineering, Malla Reddy College of Engineering for Women, Hyderabad -500100, Telangana, India

Abstract: We live in a time when technology is rapidly evolving, and cyber threats are becoming increasingly difficult to detect. Explore the leading topics of network security and learn how you can secure the Network against the most sophisticated cyber attacks. Following a successful exploit, the attacker can disable the target application. This survey provides Automated Invasion Response System (AIRS) for an understanding of different research in preserving the availability and of calculating systems in the fast-spreading invasions which demands advances in automated response ways of doing things and in detection sets of computer instructions. Response and Recovery Engine is the suggested approach for an automated response. Our system works on a game-theoretic response against fighters as modeled. The RRE understands the system-level security features by applying a method called attack-response trees (ART). Due to which RRE is responsible for any functions from attackers. The RRE works with Markov process that is automatically takes decision. We deploy fuzzy logic in process to as a result, the best response of optimization process of network actions. the RRE calculate the security metric values in network-level. In implementation of this logic, inputs to the network- level selection engine are first handled by fuzzy system which is in charge of a guessing and ranking of the possible actions. Gets involved in using its rule set of fuzzy.

INTRODUCTION

Level of intrusion in network is increasing day to day. In general, practice are classify into three broad classes.

1) Intrusion prevention methods (IPS) to handle the occurrence of attacks, e.g., network flow encryption to prevent man-in-the-middle attacks.

2) Intrusion detection systems (IDSes) Snort [2], which detects inappropriate or anonymous network related activities .

3) There are intrusion techniques to ensure safety of the computing environment which handles responsive actions based on received IDS alerts to stop attacks before they can cause significant damage. There is a delay in notification and response in this model since it is a manual process which is an advantage for attackers to hack the system and achieve their goal.

To overcome this challenge and to minimize the damage severity an automated intrusion response is in need which maintains the response to intrusion automatically. To handle this response for past few years, three types of techniques involved in enhancing automation technique to be involved in the intrusion response had been introduced. These techniques works based on the predefined mapping done using lookup table. These methods encourage response systems to deal with intrusions more faster. However, they lack in 1) mainly on flexibility since it neglects intrusion cost factor; and 2) next comes the scalability, since it is infeasible to predict, combinations from IDSes especially in a large-scale computer network. A second group of intrusion response systems (IRSes) employs a dynamic rule-based selection procedure [8] that selects response actions based on a certain attack metric, e.g., confidence or severity of attack [15].

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 after understanding the security events in the host computer using ART technique then using the other technique of Markov process it partially observes the response of the attackers. Due to which the damage caused by attackers in later period gets minimized. Once the RRE analyze the attackers' reaction in later period using this game- theoretic approach, it prevents majority damages caused by attackers. This is succeeded by taking intelligently-chosen sequence of actions.

This sequence of action takes place in RRE which has local engines within host computers and global engine, within the response and recovery server. RRE takes decision of performing global level response using global engines once the system is not recoverable by the local engines [7].

The hierarchical architecture within the server enhances the scalability, maintenance of design, and improves the performance of RRE. This helps in protecting assets in large scale network from attackers. The contributions of RRE are as follows [10]. First, RRE is responsible for any planned change in behavior usually in which the attacks stage by stage and added to it the safety measures. Second, after the knowledge of ART RRE concurrently observe uncertainties through IDS notification by Markov decision processes [11]. The imperfection expected in the suggested module is RRE certain times are not able to generate alerts for some successful intrusions. Therefore allow for this imperfection in order to be practical. RRE got through this execution successfully with a unified modeling approach in which game theory and Markov decision processes are combined. We experiment, that RRE is comparitively efficient for large networks via prototyping and experimentation rather than the critical infrastructure networks associated with the power grid. However, we believe that RRE gets suited for wide networks.

EXISTING SYSTEM

The severity of intrusions on computer networks is rapidly increasing. Previously, handling such techniques is majorly segregated into three broad classes. First, there are few methods followed to prevent intrusion which avoids the occurrence of attacks. Second, there are intrusion detection systems (IDSes), such as Snort, where inappropriate actions are being observed, for example, perceiving CrashIIS attacks by detecting malformed packet payloads [12]. Still now, most of the researches focuses mainly on preventing and detecting intrusion.

Disadvantages

- This method can be easily controlled by the attacker in turn the damage level also gets increased.
- The major disadvantage is the lack of time difference between attack and response.

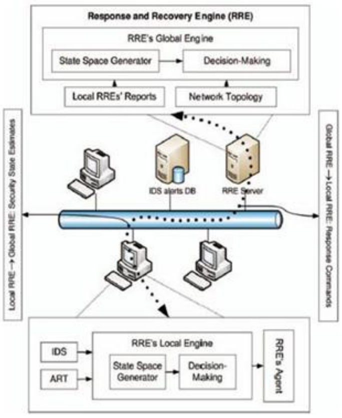
PROPOSED SYSTEM

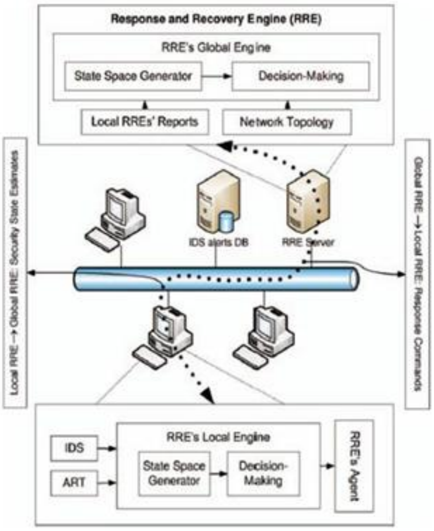
In this paper, automated cost-sensitive intrusion response system called the response and recovery engine (RRE) which is a battle between RRE and the attackers. After the implementation of this models it maintains and performs the security battle between itself and the attacker. This is achieved by a multistep, sequential, hierarchical, non zero sum. In each step of the execution, RRE observes the functionality of the intruder by ART and later by IDS system), when estimating the system's security and deciding on response actions. Due to which damage to the certain level can be eliminated.

Advantages of Proposed System

- Scalability which can be maintained for large scale computer networks.
- Segregation of high-level and low-level security issues simplifies the accurate design of response engines.

SYSTEM ARCHITECTURE





CONCLUSION

The implementation of a invasion response engine, called the Response and Recovery Engine (RRE), Simulated the environment by maintaining Stackelberg (random/including random data points) two-player game As modeled, attacker and response engine owns benefits by taking best enemy and response actions, RRE guesses the attackers functions by two level method called Attack-Response Tree (ART), and IDS alerts in guessing the security state of the system. More than that, RRE explores the (on purpose) evil and cruel attacker's next possible action space before deciding upon the best response action, so that it is that the attacker cannot cause greater damage than what RRE. Experiments show that RRE takes appropriate countermeasure actions against (happening now) attacks, and brings an insecure network to its (usual/ commonly and regular/ healthy) 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] 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] 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] 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] 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] Dean, L. Kaelbling, J. Kirman, and A. Nicholson. Planning under time constraints in stochastic domains. Artificial Intelligence, 76:35–74, 1995.

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

[10] 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.

[11] 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.

****