ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 55 – 59 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp12.pdf

FIRE: A FUZZY BASED INTRUSION RESPONSE ENGINE

T.Naresh[1], K.Guru Jyothsna Devi[2]
[1]M.Tech CSE Student, *SV College of engineering, Tirupati*, AP, India
Nareshreddy564@gmail.com
[2]Assistant Professor, Dept. of CSE, *SV College of engineering, Tirupati*, AP, India,
k.jyothsnadevi515@gmail.com

ABSTRACT

Preserving supply and integrity the of networked computing systems within the face of fast-spreading intrusions needs advances not solely in detection algorithms, however conjointly in machine-controlled response techniques. during this paper, we tend to propose a replacement approach to machine-controlled response referred to as the response and recovery engine (FIRE). Our engine employs a game-theoretic response strategy against adversaries sculptured as opponents in an exceedingly two-player Stackelberg random game. The hearth applies attack-response trees (ART) to research unwanted system-level security events inside host computers and their countermeasures victimization mathematician logic to mix lower level attack consequences. additionally, the hearth accounts for uncertainties in intrusion detection alert notifications. The hearth then chooses best response actions by resolution a partly evident competitive Markov call method that is mechanically derived from attack-response trees. To support network-level multiobjective response choice and take into account presumably conflicting network security properties, we tend to use symbolic logic theory to calculate the network-level security metric values, i.e., security levels of the system's current and probably future states in every stage of the game. specially, inputs to the network- level game-theoretic response choice engine, ar initial fed into the fuzzy system that is to blame of a nonlinear logical thinking and quantitative ranking of the potential actions victimization its antecedently outlined fuzzy rule set. Consequently, the best network-level response actions ar chosen through a game-theoretic optimisation method. Experimental results show that the hearth, victimization Snort's alerts, will shield giant networks that attack-response trees have a lot of than five hundred nodes.

Index Terms—Intrusion response systems, network state estimation, Markov call processes, random games, and symbolic logic and management

1. INTRODUCTION

The severity and range of intrusions on pc networks are apace increasing. Generally, incident- handling [1] techniques are categorized into 3 broad categories. First, there are intrusion interference strategies that take actions to stop occuFIREnce of attacks, as an example, network flow encoding to forestall man-in-the-middle attacks. Second, there ar intrusion detection systems (IDSes), like Snort [2], that try and discover inappropriate, incoFIREct, or abnormal network activities, for example, perceiving CrashIIS attacks by police investigation distorted packet payloads.

Finally, there ar intrusion response techniques that take responsive actions primarily based on received IDS alerts to prevent attacks before they\'ll cause vital harm and to make sure safety of the computing setting. So far, most analysis has centered on rising techniques for intrusion interference and detection, whereas intrusion response sometimes remains a manual method performed by network adminis- trators WHO ar notified by IDS alerts and answer the intrusions. This manual response method inevitably intro- duces some delay between notification and response, that may be simply exploited by the aggressor to reach his or her goal and considerably increase the harm [3]. Therefore, to scale back the severity of attack harm ensuing from delayed response, an automatic intrusion response is needed that provides instant response to intrusion.

We gift Associate in Nursing machine-controlled cost-sensitive intrusion response system referred to as the response and recovery engine (FIRE) that models the protection battle between itself and the aggressor as a multistep, sequential, class-conscious, nonzero- total, two-player random game. In every step of the sport, hearth leverages a replacement extended attack tree structure, referred to as the attack-response tree (ART), and received IDS alerts to judge varied security properties of the individual host systems inside the network. ARTs give a proper manner to explain host system security primarily based on potential intrusion and response eventualities for the aggressor and response engine, severally. a lot of significantly, ARTs change hearth to take into account inherent uncertainties in alerts received from IDSes (i.e., false positive and false negative rates), once estimating

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 55 – 59 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp12.pdf

the system's security and selecting response actions. Then, the hearth mechanically converts the attack- response trees into partly evident competitive Markov call processes that ar solved to realize the best response action against the aggressor, in the sense that the utmost discounted accumulative harm that the aggressor will cause later in the game is reduced. It is noteworthy that despite the mathematical value decrease in hearth that itself needs it slow to complete in apply, FIRE's final objective is to save/reduce intrusion response prices and the system damages due to attacks compared to existing intrusion response solutions. FIRE extends the state of the art in intrusion response in 3 basic ways in which. First, hearth accounts for planned adversarial behavior in that attacks occur in stages during which adversaries execute well-planned methods and address defense measures taken by system directors on the manner. It will thus by applying game theory and seeking responses that optimize on long gains. Second, hearth concuFIREntly accounts for inherent uncertain- ties in IDS alert notifications with attack-response trees born-again to a partly evident Markov call method that computes best responses despite these uncertain- ties. this is often vital as a result of IDSes nowadays and within the close to future are unable to get alerts that match absolutely to triple-crown intrusions, and response techniques should, therefore, permit for this state to be sensible. Third, for ease of style functions, hearth permits network security directors to outline high-level network security prop- erties through easy-to-understand linguistic terms for the actual target network. this is often a vital facility that hearth provides, as a result of not like system-level security properties, for example, the internet
server convenience, that will be reused across networks, the network-level security proper- ties sometimes ought to be outlined specifically for every network by the security directors manually. hearth achieves the on top of 3 goals with a unified modeling approach during which game theory and Markov call processes ar combined. we tend to demonstrate that hearth is computationally economical for comparatively giant networks via prototyping and experimentation, demonstrate that it is sensible by finding out unremarkably found facility crucial infrastruc- ture networks.

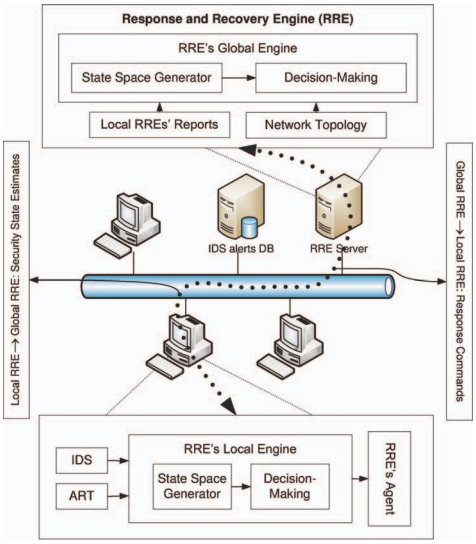

Fig. 1. High-level architecture of the FIRE.

2 RELATED WORK

EMERALD [14], a dynamic cooperative response system, introduces a stratified approach to deploy monitors through completely different abstract layers of the network. Analyzing IDS alerts and coordinative response efforts, the response elements also are able to communicate with their peers at different network layers. AAIRS [15] provides adaptation through a confidence metric related to IDS alerts and thru successful metric coFIREsponding to response actions. though EMERALD and AAIRS supply nice infrastructure for automatic government agency, they don\'t decide to balance intrusion harm and recovery value.

LADS [9], a host-based machine-controlled arms, uses a partly evident Markov call method to account for imperfect state information; but, LADS isn\'t applicable in all-purpose distributed systems attributable to their reliance on native responses and specific profile- primarily based IDS. Balepin et al. [5] address Associate in Nursing machine-controlled response-enabled system that relies on a resource sort hierarchy tree and a directed graph model referred to as a system map. each LADS and therefore the government agency in [5] are often exploited by the mortal, since none of them takes into account the malicious attacker's potential next actions whereas selecting response actions.

Game theory in Associate in Nursing IRS-related context has conjointly been utilised in previous papers. caustic and Wing [6] use a game- conjectural technique to research the protection of pc networks. The interactions between Associate in Nursing aggressor and the administrator ar sculptured as a two-player synchronic game in that every player makes selections while not the information of the methods being chosen by the opposite player; but, in reality, IDSes facilitate directors probabilisti- cally figure out what the aggressor has done before they decide upon response actions, as in consecutive games. AOAR [8], created by Bloem et al., is used to decide whether or not every attack ought to be

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 55 – 59 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp12.pdf

forwarded to the administrator or taken care of by the machine-controlled response system. Use of a single-step game model makes the AOAR vulnerable to multistep security attacks during which the aggressor considerably damages the system with Associate in Nursing showing intelligence chosen sequence of on an individual basis negligible adversarial actions.

3 FIRE's HIGH-LEVEL ARCHITECTURE

Before giving theoretical style and implementation de- tails, we offer a high-level design of fireplace, as illustrated in Fig. 1. It has 2 varieties of decision-making engines at 2 completely different layers, i.e., native and international. This data structure of FIRE's design, as mentioned later, makes it capable of handling terribly frequent IDS alerts, and selecting best response actions. Moreover, the two- layer design improves its quantifiability for large-scale pc networks, during which hearth is meant to shield an outsized range of host computers against malicious attack- ers. Finally, separation of high- and low-level security problems considerably simplifies the correct style of response engines.
At the initial layer, FIRE's native engines ar distributed in host computers. Their main inputs consist of IDS alerts and attack-response trees. All IDS alerts ar sent to and keep within the alert info (see Fig. 1) to that every native engine subscribes to be notified once any of the alerts associated with its host pc is received. it\'s noteworthy that the cuFIREnt hearth style assumes that the triggered alerts ar sure. victimization the mentioned native info, native engines figure native response actions and send them to fireplace agents that ar in charge of imposing received commands and coverage back the accomplishment standing, i.e., whether or not the command was with success carried out. The internal design of engines includes 2 major components: the state area generator, and the choice engine. Once inputs have been received, all potential cyber security states, that the host pc can be in, ar generated. The state area may well be intractably large; thus, hearth partly generates the state area so the decision-making unit will quickly decide on the best response action. The decision-making unit employs a game-theoretic algorithmic program that models attacker-FIRE interaction as a two-player game during which every player tries to maximize his or her overall profit. this suggests that, once a system is vulnerable, immediate greedy response selections don\'t seem to be essentially the simplest decisions, since they\'ll not guarantee the minimum total accumulative value concerned in complete recovery from the attack.

3.1 Local Response And Recovery

We gift the style of these elements in detail. beginning with the lowest level modules in hearth, we tend to make a case for however native engines, residing in host computers, shield native computing assets victimization security-related info, i.e., IDS alerts, concerning them.

Attack-response tree. to shield an area computing quality, its coFIREsponding native engine initial tries to figure out what security properties of the quality are profaned as results of Associate in Nursing attack, given a received set of alerts. Attack trees [6] supply a convenient manner to consistently categorise the other ways in that Associate in Nursing quality are often attacked. native engines build use of a replacement extended attack tree structure, referred to as Associate in Nursing attack- response tree (ART), that creates it potential 1) to include potential step (response) actions against attacks, and 2) to contemplate intrusion detection uncertainties due to false positives and negatives in police investigation triple-crown intru- sions, whereas estimating the cuFIREnt security state of the system. The attack-response trees ar designed offline by specialists for every computing quality, for example, Associate in Nursing SQL server, residing in an exceedingly host pc. it\'s vital to notice that, not like the attack tree that is intended per all potential attack eventualities, the ART model is made primarily based on the attack consequences, for example, Associate in Nursing SQL crash; so, the designer will not have to take into account all potential attack eventualities that may cause those consequences.
Stackelberg game: hearth versus aggressor. Reciprocal interac- tion between the mortal and response engine in a computing system may be a game in that every player tries to maximise his or her own profit. The response choice method in hearth is sculptured as a consecutive Stackelberg random game [9] during which hearth acts because the leader whereas the aggressor is the follower; but, in our infinite-horizon game model, their roles might amendment while not poignant the ultimate answer to the matter.

A distinct competitive {markovian|Markovian|stochastic method} call process is outlined as a tuple ðS; A; r; P ; Þ wherever S is the security state area, assumed to be Associate in Nursing absolute nonempty set leaf consequence nodes within the ART graph beneath considera- tion. In different words, as a binary string, every MDP security state vector represents the ART leaf node consequences that have already been set to one per the received alerts from IDS systems. for example, Associate in Nursing ART graph with n leaf nodes results in a generated MDP model with 2n security states, i.e., n-bit vectors. For ART graphs with an outsized range of leaf nodes, this exponential growth of the protection state area sometimes results in the state area explosion downside, that hearth deals with by creating use of approximation techniques.

3.2 Global Response And Recovery

Although host-based intrusion response is taken into consideration by FIRE's native engines victimization native ART graphs and the IDS rule-set for computing assets, as an example, the SQL server, maintenance of worldwide network-level security security level otherwise.

ISSN 2347 - 3983

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 55 – 59 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp12.pdf

To address the above-named challenges in assessing the international security properties for the whole network given the time period reports from native response engines, we tend to propose a multiobjective network security reward operate S ! ½0; one (see Section five.2) that uses a fuzzy logic-based controller to calculate, at every time instant, a security live worth for the whole network. Throughout this paper, we are going to target the generic security property of "Is the network cuFIREntly secure?". All different network-level security properties are often calculated equally.

4. FUZZIFICATION OF THE LOCAL ENGINE REPORTS

Fuzzy sets ar sometimes outlined by their membership functions that describe the understanding that a part belongs to the set as hostile the normal binary set member- ships. For instance, a fuzzy membership may quantify whether or not (or a lot of exactly, however much) any system state of affairs (belief state) is a member of the network international security set. The fuzzification block converts the fuzzy system inputs, i.e., g 's from native engines, to fuzzy sets that ar used by the fuzzy system's logical thinking engine later. Similar to [12], hearth uses mathematician and triangular member- ship functions. specially, we tend to outline l ð g Þ to represent the degree that g is low, i.e., belongs to the low set. And m ð:Þ and h ð:Þ membership functions ar equally outlined for the medium and high sets. In this section, we tend to investigate however the planned response and recovery engine performs in reality. we tend to have imple- mented hearth on prime of Snort two.7 [2], that is Associate in Nursing ASCII text file signature-based IDS. The experiments were run on a computing system with a two.2-GHz AMD Athlon sixty four Processor 3700 þ with one MB of cache, two GB of memory, and the
Ubuntu (Linux two.6.8-9) package. Model generation performance. though network opology Associate in Nursingalyses and CMDP model generation in hearth is performed throughout an offline section, for sensible usages, it is still vital to complete those steps inside an inexpensive amount. To validate FIRE's potency on varied networks with completely different sizes and topologies, we tend to measured however long hearth takes to generate the CMDP model for haphazardly generated networks. Figs. 5a and 5b show the CMDP generation time demand and the model's size. The results were averaged over one,000 runs. As illustrated, for large-scale power networks with 330K host computers, hearth analyzed the inputs and generated the CMDP model inside eight milliseconds.
Response optimisation quantifiability. To measure however hearth handles advanced networks consisting of an outsized range of host systems, we tend to measured the time needed by hearth to figure the best response action versus varied metrics. Fig. 6d shows the average time-to-response over 10 runs versus the attack-response tree order, i.e., the utmost range of youngsters for every node.2 for every tree order d, a balanced tree, during which every node has d kids, is generated; gates ar assigned to be AND or OR with equal chance, i.e., 0.5. The \"-optimality termination criterion in Bellman's equation and discounting issue were set to \" ¼ 0:1 and ¼ 0:99, severally. Then, a call method is made and solved , and the total time spent is recorded increasing the ART order leads to speedy growth of the desired time-to-response by the response engine.
In another quantifiability analysis experiment, we tend to measured time-to-response versus the range of nodes in balanced ART trees of order two. Fig. half-dozen shows average results on ten runs for 3 eventualities. First, given IDS alerts and therefore the ART tree, the entire call model consisting of all states in the state area was made. As shown in Fig. 6a, the response engine will solve for best response actions for ART trees with up to forty five nodes inside concerning two minutes. Second, Associate in Nursing on-line finite-lookahead stochastic process call model with Associate in Nursing growth limit of 4 steps was generated and solved . As illustrated in Fig. 6b, restricted growth improves a solution's convergence speed and will increase the soluble ART size to trees with up to one hundred fifteen nodes inside thirty seconds. Third, to additional improve FIRE's quantifiability, we tend to evaluated however quick a call method is solved with Associate in Nursing higher growth limit of two. Fig. 6c shows that ART trees with a lot of than 900 nodes ar still soluble in less than forty seconds. By resolution ART trees with concerning 900 nodes in a minute, hearth will shield large-scale pc networks. Comparison.
We sculptured the aggressor to be fully intelligent; in different words, in every step, he or she took the foremost harmful potential adversarial action. There were a complete of sixty four beginning eventualities (states) for 2 completely different game schemes. In the initial theme, the action magnitude relation between government agency and the aggressor was 1; in different words, for every action taken by the response system, the aggressor was allowed to choose one adversarial action. for sure, for all initial eventualities, in selecting the best action, hearth needed a recovery value but or equal to what the static government agency did. within the second game theme, we tend to fortified the attacker's strength, and set the action magnitude relation to 1/2 that means that for every action by the government agency, the aggressor was allowed to require 2 actions. In 5 eventualities (out of 64), hearth caused a lot of recovery value than its static rival, {the reason|the magnitude relationnale|the explanation} being that the hearth chooses the best response action beneath the idea that the action ratio is one.

5. CONCLUSION:

. we tend to propose a replacement approach to machine-controlled response referred to as the response and recovery engine (FIRE). Our engine employs a game-theoretic response strategy against adversaries sculptured

International Journal of Emerging Trends in Engineering Research (IJETER), Vol. 3 No.6, Pages : 55 – 59 (2015)
Special Issue of NCTET 2K15 - Held on June 13, 2015 in SV College of Engineering, Tirupati
http://warse.org/IJETER/static/pdf/Issue/NCTET2015sp12.pdf

as opponents in an exceedingly two-player Stackelberg random game. The hearth applies attack-response trees (ART) to research unwanted system-level security events inside host computers and their countermeasures victimization mathematician logic to mix lower level attack consequences. additionally, the hearth accounts for uncertainties in intrusion detection alert notifications. The hearth then chooses best response actions by resolution a partly evident competitive Markov call method that is mechanically derived from attack-response trees. To support network-level multiobjective response choice and take into account presumably conflicting network security properties, we tend to use symbolic logic theory to calculate the network-level security metric values, i.e., security levels of the system's current and probably future states in every stage of the game.

6. RE FERENCES

[1] B. Foo, M. Glause, G. Howard, Y. Wu, S. Bagchi, and E. Spafford, info Assurance: reliableness and Security in Networked Systems. Morgan Kaufmann, 1507.
[2] R. Rehman, Intrusion Detection Systems with Snort. Prentice-Hall, 1503.
[3] F. Cohen, "Simulating Cyber Attacks, Defenses, and Conse- quences," http://all.net/journal/ntb/simulate/simulate.html, 1499.
[4] S.A. Zonouz, H. Khurana, W.H. Sanders, and T.M. Yardley, "FIRE: A Game-Theoretic Intrusion Response and Recovery Engine," Proc. IEEE/IFIP Int'l Conf. Dependable Systems and Networks (DSN), pp. 439-448, 1509.
[5] 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. 1503.
[6] B. Schneier, Secrets and Lies: Digital Security in an exceedingly Networked World. John Wiley & Sons, 1500.
[7] A. Valdes and K. Skinner, "Adaptive, Model-Based observance for Cyber Attack Detection," Proc. Recent Advances in Intrusion Detection, pp. 80-92, 1500.
[8] C. Kruegel, W. Robertson, and G. Vigna, "Using Alert Verification to spot triple-crown Intrusion makes an attempt," IP and Comm., vol. 27, pp. 95-58, 1504.
[9] G. Owen, theory of games. educational Press, 1495.
[10] J. fibre and K. Vrieze, Competitive Markov call Processes. Springer-Verlag, 1497.
[11] S. Hsu and A. Arapostathis, "Competitive Markov call Processes with Partial Observation," Proc. IEEE lnt'l Conf. Systems, Man and Cybemetics, vol. 1, pp. 66-81, 1504.
[12] L. Kaelbling, M. Littman, and A. Cassandra, "Partially evident Markov call Processes for Artificial Intelligence," Proc. German Conf. computer science: Advances in Artificial Intelligence, vol. 981, pp. 1-12, 1495.
[13] E. Sondik, "The best management of partly evident Markov Processes," Ph.D. thesis: Standford Univ., 1471.
[14] R. Bellman, Dynamic Programming, Princeton Univ. Press, 1457.
[15] D.F. Jenkins and K.M. Passino, "An Introduction to nonlinear Analysis of Fuzzy management Systems," J. Intelligent and Fuzzy Systems, vol. 7, no. 1, pp. 75-103, http://dl.acm.org/itation.cfm