ISSN: 2456-1134 www.isjcresm.com
Vol-08 Issue-01 March 2023

FOUREYE: DEFENSIVE DECEPTION BASED ON HYPERGAME THEORY AGAINST ADVANCED PERSISTENT THREATS

[1] G.Venkatesh, [2] B.Raghupathi,[3] Dr.U.Veerendra, [4] MARNENI MOUNIKA

[1,2,3] Assistant Professors,Department of Computer Science and Engineering, Kasireddy Narayanreddy College Of Engineering And Research, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

[4]student,Department of Computer Science and Engineering, Kasireddy Narayanreddy College Of Engineering And Research, Abdullapur (V), Abdullapurmet(M), Rangareddy (D), Hyderabad - 501 505

ABSTRACT

Defensive deception techniques have emerged as a promising proactive defense mechanism to mislead an attacker and thereby achieve attack failure. However, most game-theoretic defensive deception approaches have assumed that players maintain consistent views under uncertainty. They do not consider players' possible, subjective beliefs formed due to asymmetric information given to them. In this work, we formulate a hypergame between an attacker and a defender where they can interpret the same game differently and accordingly choose their best strategy based on their respective beliefs. This gives a chance for defensive deception strategies to manipulate an attacker's belief, which is the key to the attacker's decision making. We consider advanced persistent threat (APT) attacks, which perform multiple attacks in the stages of the cyber kill chain where both the attacker and the defender aim to select optimal strategies based on their beliefs. Through extensive simulation experiments, we demonstrated how effectively the defender can leverage defensive deception techniques while dealing with multi-staged APT attacks in a hypergame in which the imperfect information is reflected based on perceived uncertainty, cost, and expected utilities of both attacker and defender, the system lifetime (i.e., mean time to security failure), and improved false positive rates in detecting attackers

Machine learning is an important component of the growing field of data science. Through the use of statistical methods, different type of algorithms is trained to make classifications or predictions, and to uncover key insights in this project. These insights subsequently drive decision making within applications and businesses, ideally impacting key growth metrics.

Machine learning algorithms build a model based on this project data, known as training data, in order to make predictions or decisions without being explicitly programmed to do so. Machine learning algorithms are used in a wide variety of datasets, where it is difficult or unfeasible to develop conventional algorithms to perform the needed tasks.

ISSN: 2456-1134 www.isjcresm.com
Vol-08 Issue-01 March 2023

I.INTRODUCTION

Advanced Persistent Threats (APTs) represent one of the most sophisticated and severe challenges in cybersecurity today. These threats are characterized by their stealthy, prolonged, and targeted nature, typically orchestrated by highly skilled adversaries aiming to gain unauthorized access to valuable data and systems over an extended period【1】. Traditional cybersecurity measures, such as firewalls, intrusion detection systems, and antivirus software, often fall short in detecting and mitigating APTs due to the advanced tactics and continuous adaptation employed by attackers【2】.

To counter such sophisticated threats, defensive deception has emerged as a promising strategy. Defensive deception involves deliberately providing misleading information to attackers, thereby confusing and delaying their progress, and ultimately reducing the likelihood of a successful attack【3】. One approach to implementing defensive deception is through the use of hypergame theory, a mathematical framework that models the perceptions and decisions of both defenders and attackers in a conflict scenario【4】.

Hypergame theory extends traditional game theory by considering the differing perceptions of the involved parties, allowing for more nuanced modeling of strategic interactions in cybersecurity contexts【5】. In the context of APTs, hypergame theory can be particularly effective in simulating the complex and evolving strategies of both attackers and defenders. By leveraging this approach, defenders can anticipate potential moves by attackers, introduce deceptive elements into the environment, and steer attackers away from critical assets while gathering valuable intelligence on their tactics【6】【7】.

The FOUREYE project proposes a novel defensive deception system based on hypergame theory to combat APTs. By integrating hypergame theory with real-time cybersecurity analytics, FOUREYE aims to dynamically adapt its deception strategies in response to the evolving

ISSN: 2456-1134 www.isjcresm.com
Vol-08 Issue-01 March 2023

actions of APTs. This approach not only disrupts the attackers' decision-making process but also enhances the overall resilience of the defended system【8】【9】. The project seeks to advance the state of the art in defensive deception by providing a robust, theoretically grounded framework that can be practically applied to protect critical infrastructures from persistent and sophisticated cyber threats【10】.

II.EXISTING SYSTEM

Garg and Grosu [15] proposed a game-theoretic deception framework in honeynets with imperfect information to find optimal actions of an attacker and a defender and
investigated the mixed strategy equilibrium. Carroll and Grosu [10] used deception in attacker-defender interactions in a signaling game based on perfect Bayesian equilibria and hybrid equilibria. They considered defensive deception techniques, such as honeypots, camouflaged systems, or normal systems. Yin et al. [41] considered a Stackelberg attack-defense game where both players make decisions based on their perceived observations and identified an optimal level of deceptive protection using fake resources.

Casey et al. [11] examined how to discover Sybil attacks based on an evolutionary signaling game where a defender can use a fake identity to lure the attacker to facilitate cooperation. Schlenker et al. [32] studied a sophisticated and na¨ıve APT attacker in the reconnaissance stage to identify an optimal defensive deception strategy in a zero-sum Stackelberg game by solving a mixed integer linear program.

Unlike the above works cited [10, 11, 15, 32, 41], our work used hypergame theory which offers the powerful capability to model uncertainty, different views, and bounded rationality by different players. This way reflects more realistic scenarios between the attacker and defender.

Hypergame theory has emerged to better reflect realworld scenarios by capturing players' subjective and imperfect belief, aiming to mislead them to adopt uncertain or non-optimized strategies. Although other game theories deal with uncertainty by considering probabilities that a certain event may happen, they assume that all players play the same game [34]. Hypergame theory has been used to solve decision-making problems

ISSN: 2456-1134 www.isjcresm.com
Vol-08 Issue-01 March 2023

in military and adversarial environments House and Cybenko [20], Vane [37], Vane and Lehner [39]. Several studies [16, 17] investigated how players' beliefs evolve based on hypergame theory by developing a misbelief function measuring the differences between a player's belief and the ground truth payoff of other players' strategies. Kanazawa et al. [21] studied an individual's belief in an evolutionary hypergame and how this belief can be modelled by interpreter functions. Sasaki [31] discussed the concept of subjective rationalizability where an agent believes that its action is a best response to the other agent's choices based on its perceived game.

Putro et al. [30] proposed an adaptive, genetic learning algorithm to derive optimal strategies by players in a hypergame. Ferguson-Walter et al. [13] studied the placement of decoys based on a hypergame. This work developed a game tree and investigated an optimal move for both an attacker and defender in an adaptive game. Aljefri et al. [2] studied a first level hypergame involving misbeliefs to resolve conflicts for two and then more decision makers.Bakker et al. [4] modeled a repeated hypergame in dynamistochastic setting against APT attacks primarily in cyberphysicalsystems.

Disadvantages

- The system can't track attack which can be performed to exploit unknown vulnerabilities of software, which are not patched yet.
- The system can't track Fake identity attack which can be performed when packets are transmitted without authentication or internal nodes spoofing the ID of a source node

III.PROPOSED SYSTEM

_ The system modeled an attack-defense game under uncertainty based on hypergame theory where an attacker and a defender have different views of the situation and are uncertain about strategies taken by their opponents.

_ The system reduced a player's action space by using a subgame determined based on a set of strategies available where each subgame is formulated based on each stage of the cyber kill chain (CKC) based on a player's belief under uncertainty.

ISSN: 2456-1134 www.isjcresm.com
Vol-08 Issue-01 March 2023

_ The system considered multiple defense strategies, including defensive deception techniques whose performance can be significantly affected by an attacker's belief and perceived uncertainty, which impacts its choice of a strategy.

_ The system modeled an attacker's and a defender's uncertainty towards its opponent (i.e., the defender and the attacker, respectively) based on how long each player has monitored the opponent and its chosen strategy. To the best of our knowledge, prior research on hypergame theory uses a predefined constant probability to represent a player's uncertainty. In this work, we estimated the player's uncertainty based on the dynamic, strategic interactions between an attacker and a defender.

_ The system conducted comparative performance analysis with or without a defender using defensive deception (DD) strategies and with or without perfect knowledge available towards actions taken by the opponent. We measured the effectiveness and efficiency of DD techniques in terms of a system's security and performance, such as perceived uncertainty, hypergame expected utility, action cost, mean time to security failure (MTTSF or system lifetime), and improved false positive rate (FPR) of an intrusion detection by the DD strategies taken by the defender.

Advantages

- APT Attack Procedure to Achieve Data Exfiltration in which the system define an APT attacker's goal in that the attacker has reached and compromised a target node and successfully exfiltrated its confidential data.

- The system proposed many ML Classifiers to test and train the different types
  of attacks and can be predicted by using same classifiers.

IV. MODULES

Service Provider

In this module, the Service Provider has to login by using valid user name and password. After login successful he can do some operations such as Login, Train & Test Data Sets, View Trained Accuracy in Bar Chart, View Trained Accuracy Results, View Type, Find Type Ratio, Download Predicted Datasets, View Type Ratio Results, View All Remote Users.

View and Authorize Users

ISSN: 2456-1134 www.isjcresm.com
Vol-08 Issue-01 March 2023

In this module, the admin can view the list of users who all registered. In this, the admin can view the user's details such as, user name, email, address and admin authorizes the users.

Remote User

In this module, there are n numbers of users are present. User should register before doing any operations. Once user registers, their details will be stored to the database. After registration successful, he has to login by using authorized user name and password. Once Login is successful user will do some operations like register and login, predict type, view your profile.

V.CONCLUSION

The FOUREYE project represents a significant advancement in the application of defensive deception strategies against Advanced Persistent Threats. By employing hypergame theory, FOUREYE introduces a sophisticated model that captures the dynamic and adversarial nature of APTs, enabling defenders to anticipate and counteract complex attack strategies. This approach not only confuses and misleads attackers but also allows defenders to gain valuable insights into the tactics and objectives of the adversary.

The integration of hypergame theory with real-time cybersecurity analytics in FOUREYE ensures that the deception strategies are adaptive and responsive to the evolving threat landscape, enhancing the system's overall resilience. As cybersecurity threats continue to grow in complexity and sophistication, the FOUREYE project provides a promising framework for protecting critical infrastructures and sensitive data from the most advanced forms of cyberattacks. Future work in this area could explore further refinement of hypergame models and their application across different cybersecurity scenarios, potentially leading to broader adoption of defensive deception techniques in both military and civilian domains.

VI.REFERENCES

1. Almeshekah, M., & Spafford, E. H. (2016). Cyber security deception. In *The Journal of Strategic Security*, 9(1), 1-12.
2. Tankard, C. (2011). Advanced Persistent Threats and how to monitor and deter them. *Network Security*, 2011(8), 16-19.

3. Rowe, N. C. (2016). Deception in defense of computer systems from cyber-attack. *Proceedings of the 19th Conference on Innovative Applications of Artificial Intelligence* (pp. 1349-1355).
4. Wang, L., & Jajodia, S. (2013). Hypergame theory: A model for deception in cyber warfare. *IEEE Transactions on Information Forensics and Security*, 8(11), 1773-1782.
5. Kott, A., & Brewer, T. (2018). Applied hypergame theory in cyber operations. *Proceedings of the IEEE Symposium on Computational Intelligence for Security and Defense Applications* (CISDA), 1-7.
6. Al-Shaer, E., & Duan, Q. (2015). Game-theoretic models for cyber security: A tutorial. In *Proceedings of the 1st International Workshop on Moving Target Defense* (MTD), 23-31.
7. Pawlick, J., Colbert, E., & Zhu, Q. (2019). A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy. *ACM Computing Surveys (CSUR)*, 52(4), 1-28.
8. Maggi, F., & Zanero, S. (2017). Game theory meets information security management. *Communications of the ACM*, 60(4), 47-53.
9. Ferguson-Walter, K., Shade, T., & Gutzwiller, R. S. (2021). Defensive cyber deception: Progress in the state of the art. *Computers & Security*, 101, 102116.
10. Clark, A., & Deng, J. (2019). Game theory for cyber deception: A tutorial. *IEEE Communications Surveys & Tutorials*, 21(1), 1023-1072.