Foureye Defensive Deception Against Advanced Persistent Threats via Hypergame Theory

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

**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 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

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.

\_ 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.

**SYSTEM REQUIREMENTS**

➢ **H/W System Configuration:-**

➢ Processor - Pentium –IV

➢ RAM - 4 GB (min)

➢ Hard Disk - 20 GB

➢ Key Board - Standard Windows Keyboard

➢ Mouse - Two or Three Button Mouse

➢ Monitor - SVGA

**SOFTWARE REQUIREMENTS:**

* **Operating system :** Windows 7 Ultimate.
* **Coding Language :** Python.
* **Front-End :** Python.
* **Back-End :** Django-ORM
* **Designing :** Html, css, javascript.
* **Data Base :** MySQL (WAMP Server).