ADAPT: A Game Inspired Attack-Defense and Performance Metric Taxonomy

Chris Simmons, Sajjan Shiva, Harkeerat Bedi, Vivek Shandilya

ADAPT: A Game Inspired Attack-Defense And Performance Metric Taxonomy

Chris B. Simmons, Sajjan G. Shiva, Harkeerat Bedi, Vivek Shandilya

University of Memphis, Computer Science Department, Memphis, Tennessee
{cbsmmons, sshiva, hsbedi, v.shandilya}@memphis.edu

Abstract. Game theory has been researched extensively in network security demonstrating an advantage of modeling the interactions between attackers and defenders. Game theoretic defense solutions have continuously evolved in most recent years. One of the pressing issues in composing a game theoretic defense system is the development of consistent quantifiable metrics to select the best game theoretic defense model. We survey existing game theoretic defense, information assurance, and risk assessment frameworks that provide metrics for information and network security and performance assessment. Coupling these frameworks, we propose a game theoretic approach to attack-defense and performance metric taxonomy (ADAPT). ADAPT uses three classifications of metrics: (i) Attacker, (ii) Defender (iii) Performance. We proffer ADAPT with an attempt to aid game theoretic performance metrics. We further propose a game decision system (GDS) that uses ADAPT to compare competing game models. We demonstrate our approach using a distributed denial of service (DDoS) attack scenario.

Keywords: Game Theory, Taxonomy, Security Management

1 INTRODUCTION

Game theory has received increased attention from network security researchers, investigating defense solutions. The game theory approach has the advantage of modeling the interactions between attackers and defenders, where players have the ability to analyze other player's behavior. This may enable an administrator to develop better strategic defenses for the system. For instance, when there are many actions available to the attacker and defender, it becomes difficult to develop solution strategies. Hamilton, et al. [1] outlined the areas of game theory which are relevant to information warfare using course of actions with predicted outcomes and what-if scenarios. Jiang, et al. [2] proposed an attack-defense stochastic game model to predict the next actions of an attacker using the interactions between an attacker and defender. Therefore, it is vital to provide a network administrator the capability to compare multiple strategies using the appropriate metrics to optimize the network.

In this work we consider various metrics for game theoretic models. Bellovin [3] inferred that designing proper metrics for security measurement is a tough problem that should not be underestimated. Current research is lacking in terms of providing information a system administrator can use in determining metrics to quantify performance of diverse game theoretic defense models. One of the problems faced by research pertaining to security games is how to evaluate different network security game models, in terms of performance, accuracy, and effectiveness. The Institute for Information and Infrastructure Protection (I3P) has identified security metrics as priority for current research and development [4]. We extend this notion to provide a comprehensive taxonomy to aid in assessing the overall performance and quality of a game theoretic model. Prior game theoretic research mainly focused on classifying metrics based on a distribution of games across various game types and models. Further, the game theoretic defense mechanisms in literature are arbitrary and ad hoc in nature. This makes game theoretic defense models very complex and designed towards application specific scenarios [5]. We propose an alternative real world approach by classifying our metrics based on a real world distributed denial of service (DDoS) scenario.

In this paper, we attempt to address limitations in research through the proposed game theoretic attack-defense and performance metric taxonomy (ADAPT), which is a taxonomy of game related metrics. We define a game as the interactions between two players with conflicting goals. In our case these players are the attacker (hacker) and system administrator (defender). Game metrics are a set of tools which are used to measure the various kinds of impact a game model has on each of its players. We classify these game metrics based on their impact on attacker, defender, and the performance of the game model on the system which is being run. Prior research has shown, with the use of game theory, how the interaction should take place based on the strategy and the strategy selected from the game model. In this traditional scenario one game model is assessed relative to a particular attack. He, et al. [6] proposed a Game Theoretical Attack-Defense Model (GTADM), similar to ADAPT, that quantifies the probability of threats in constructing a risk assessment framework. We extend these general game theory steps and concepts proposed in He, et al. [6] with the use of ADAPT being able to assess competing game models and select the game model which is suitable for defense. This provides a defender with a preliminary view of multiple game models associated to a particular attack.

This research is composed of attack attributes and associated metrics that can be used to assess and compare competing game models. Thus, ADAPT provides a metric-centric approach to selecting the optimal game model. A game model is to evaluate the security level, performance, and quality of a system that will aid in selecting the appropriate game defense model at a specific time of the game. These metrics belong to different game theoretic defense models, information assurance, and risk assessment frameworks. Prior work towards developing a security metric taxonomy focuses on three core relationships of metric classifications involving organization, operation, and technical [7, 8, 9]. In proposing ADAPT, we focus on metrics with technical association.

This paper is organized as follows: In section 2 we provide a motivating scenario and in section 3 we define characteristics for good security metrics followed by our proposed metric taxonomy. In section 4 we define the metrics used in a game inspired attack-defense and performance metric taxonomy. In section 5 we introduce a game model comparing system based on ADAPT and the methodology used to map metrics within ADAPT, followed by ADAPT applied within the Game Inspired Defense Architecture (GIDA). In section 6 we provide a brief literature review on performance and security metrics. In section 7, we conclude our paper and highlight future work.

2 MOTIVATING SCENARIO

In this section we start with a brief overview of game theory concepts and provide a motivating example, which highlight the relationship to the proposed metrics that will assess game defense models. There are four basic concepts of Game Theory : (i) ***A player*** is the basic entity of a game who decides to perform a particular action (ii) ***A game*** is a precise description of the strategic interaction that includes the constraints of, and payoffs for, actions that the players can take, but does not correspond to actual actions taken (iii) ***A strategy*** for a player is a complete plan of actions in all possible situations throughout the game (iv) ***A Nash equilibrium*** is a solution concept that describes a steady state condition of the game; no player would prefer to change his strategy as that would lower his payoffs given that all other players are adhering to the prescribed strategy. Roy, et al. [10] surveyed existing game theoretic solutions designed to enhance network security. They emphasized that Game Theory has the advantage of treating explicitly intelligent decision makers having divergent interests.

Now, let us consider a scenario, in which a DDoS attack is taking place. There are multiple game models to choose for defense, but the defender is unsure which model has performed the best historically to make a determination. The defender can view the strategy spaces of all the games associated to the DDoS attack; however it will take the defender a significant amount of time to select the best game available. In modeling such player strategies, the DDoS attack presents a challenging scenario, which has increased in sophistication [11] and motivates our research in this paper. Although research has evolved relative to the DDoS attack, it is continuously a scenario that deserves much attention due to its simplicity and dominate nature of coordinated botnet use [12] to cause an enormous amount of damage. Moreover, the punishment relative to a DDoS attack is minimal to non-existent. Typically, when a DDoS attack takes place in the real world, attackers lease nodes to conduct an attack against a target, or set of targets. Once the attack is complete, the leased nodes are returned to the pool; where another party will lease those nodes allowing a constant change in IP addresses. Due to the nature of the DDoS attack, the most common defense against DDoS attacks is to block nodes. Parameswaran, et al. [13] utilized blocklist as a defense mechanism in a spammer's game theoretic model. Majority of the DDoS attacks are just blocked, which does not sustain a punitive cost and punishment by legal action is rare.

Therefore, in this work the DDoS example is considered by and large a static one shot game to provide an intuitive example of how the proposed taxonomy can be implemented within a system. When we look at network attacks in general, there are fundamental components that are likely present in a DDoS attack. Mirkovic and Reihner [11] echoed this point by placing emphasis on crucial features of an attack to comprehend the detailed differences. Hence, we believe the network has some tangible attack components that will allow experiential knowledge mapping to ADAPT metrics. The goal is to produce a summary of metrics, which will in turn be used to determine the best game model pursuant to the metrics selected within the ADAPT framework. Thus answering the question from Mirkovic and Reihner [11], how would two different defense models perform under a given attack? We represent a generalization of how each attribute will be mapped to the attacker, defender, and the performance of the target system. The scope of this work investigates metrics selected based on experiential knowledge, as opposed to metrics autonomously selected by the system.

Continuing our scenario, an attacker initiating a DDoS attack acquires a number of nodes to conduct the attack. This increases the amount of bandwidth consumed by the attacker and introduces an increase in the attacker's probability of being caught by the defender. We observe by generalizing attack components and associating them to game inspired metrics, where we are able to provide an overview of game model performance. This enables the defender to select the optimal game model for defense. We further illustrate our scenario in section 5.

3 CHARACTERISTICS OF GAME INSPIRED METRICS

We use characteristics of security metrics to further assist with evaluating metrics for game theoretic defense models. A performance study requires a set of metrics to be chosen for analysis [7]. Performance analysis requires comparing two or more systems and finding the best among them [7]. We extend this to game theoretic defense models, where the network administrator has the ability to select the best game suitable for optimal defense at a specific time. With a dynamic selection process of the best game permits a network administrator to systematically choose a defense solution applicable for defense. The game selection is based on the knowledge of how well a game model represents the considered security situation. Our methodology of game model selection is highlighted in section 5.

There is increased research involving the development of taxonomy for security metrics, where characteristics are provided to ensure organizations understand the metrics when quantifying and evaluating security. Understanding the metrics require a distinction between metric and measurement. Metrics are the resultant of a comparison of two or more baseline measurement over time, whereas measurement is a single point in time view of specific factors [14]. Swanson [15] defined a metric as tools designed to facilitate the appropriate decision for a specific situation, improve performance and accountability through collection, analysis, and reporting of pertinent performance information.

In the Federal Plan for Cyber security and Information Assurance Research and Development of 2006, the National Science and Technology Council (NSTC) has recommended developing information assurance metrics as a priority in federal agencies [16]. Vaughn et al. [17] described one of the pressing issues involving security engineering is the adoption of measures or metrics that can reliably depict hardware and software system assurance. Research has suggested the characteristics of good metrics [7, 8, 14, 15, 17]. We encompass a list of metric characteristics from literature that provides a foundation to develop comprehensive game theoretic defense taxonomy. Wesner [9] introduced the concept of a metric being S.M.A.R.T.(specific, measurable, actionable, relevant, timely). Manadathata and Wing [18] described a system action can potentially be part of an attack, and hence contributes to attack surface, which also includes the contribution of system resources. We use the notion for validation of our game theoretic defense architecture to measure which game is providing a higher level of security compared to another.

Applying relevant metric characteristics from research illustrates our proposed game inspired approach to an attack-defense and performance metric taxonomy ADAPT (Figure 1). As mentioned earlier, it utilizes three classifications of metrics: attacker, defender, and performance. ADAPT enables a network administrator to view and apply pertinent metrics to evaluate performance in multiple security games.

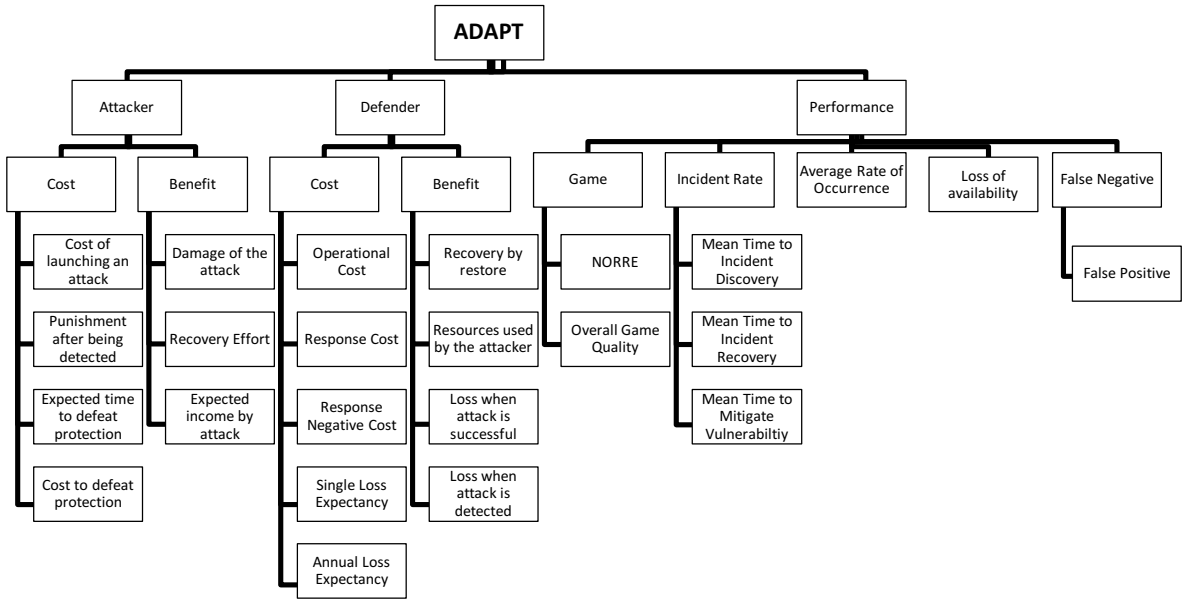

Fig. 1. Attack-Defense And Performance metric Taxonomy (ADAPT)

4 ADAPT: ATTACK-DEFENSE AND PERFORMANCE METRIC TAXONOMY

As seen from (Figure 1), ADAPT produces relevant metrics to assign values to the components of the attack-defense cost and benefit as well as the performance. These metrics and their calculations are determined based on a review of literature. We utilized these metrics from literature being the same domain in which relevance is closely related to cyber security. An information security measurement standard provides insight to how well a system is performing and analyze whether investments, in information security, are beneficial. Potential benefits include increasing information security performance and providing quantifiable inputs for investment.

We identify, in ADAPT, the following three classifiers: (i) Attacker, (ii) Defender (iii) Performance. We assume that these metrics are generic and not specific for a particular game. The attacker and defender metrics have relation to the game models. The performance metrics are used separately from the defender metrics, mainly because the performance metrics have association to the performance of the game model as a whole. Furthermore, the performance metrics relate to the performance of the system in which the game model is run. Its classification provides additional information associated to the game that will assist a defender in selecting the optimal competing game models for defense.

4.1 Attacker Metrics

In this section we provide insight into the metrics selected regarding the cost and benefit from the perspective of the attacker.

Cost of Attacker. The cost of an attacker to attack a specific target can be divided into the following metrics.

He et al. [6] used cost of launching an attack and punishment to the attacker as metrics to define the cost of attack.

- **Cost of launching attack (COLA):** Consists of money and time that an attacker can pay in order to launch an attack against a target.
- **Punishment after being detected (PABD):** Consists of the legal loss of the attacker, which involves one of the metrics used to define the cost of an attacker.

He et al. [6] used four instances in game scenarios involving non-cooperative non-zero-sum static game with complete information, where the relations between Strategy Profile and attacker cost are:

- When the attacker and defender both take actions:

$$Cost\ of\ attacker = COLA + P \times PABD \quad (1)$$

P is the detection rate of attacks.

- When the attacker takes an action and the defender does not:

$$Cost\ of\ attacker = COLA \quad (2)$$

- When the attacker does not take an action and the defender takes an action:

$$Cost\ of\ attacker = 0 \quad (3)$$

- When the attacker and defender do not take an action:

$$Cost\ of\ attacker = 0 \quad (4)$$

Carin et al. [19] proposed the following metrics to cyber risk assessment evaluating the Attack/Protect Model. These metrics are based on generating a probability distribution for cost, in terms of time, of successfully defeating the protections applied to critical intellectual property (IP).

- **Expected cost of defeating a protection (ECDP):** Involves the cost in man hours an attacker would exhibit to successfully defeat the protection. The probability distribution (Pr) is based on historical data of successfully attacking the IP. The cost of the ith man-hour in the attack is denoted by (c_i).

$$\sum_{i=0}^{\infty} c_i\, Pr(i) \quad (5)$$

- **Expected time to defeat the protection (ETDP):** Involves the hours an attacker contributes to successfully defeat the protection. The probability distribution (Pr) is based on historical data of successfully attacking the IP.

$$\sum_{i=0}^{\infty} i\, Pr(i) \quad (6)$$

Benefit of Attacker. Benefit of attacker entails the benefit the attacker receives when implementing an attack against a specific target (i.e. Fame or Monetary Value). Below we provide various metrics from literature assessing benefit of attacker.

Lye [20] divided the benefit of an attacker into the following metrics. Although the parameters used calculate the benefit, it can be inferred with an example (e.g. the damage can involve the reduced bandwidth of a system due to a DoS attack, whereas the recovery effort a network administrator puts forth in the amount of time to bring the system to its original state prior to the attack).

- **Damage of the attack (DOA):** Consists of the degree of damage in which the attacker is able to cause on the target system.
- **Recovery effort (time) required by defender (RERD):** Involves the time it takes for a defender to bring the system to a safe state of execution.
- **Expected income by the attacker (EIBA):** Involves the monetary value received by the attacker when an attack is successful. This value can be computed using the amount of effort exhibited by the defender in terms of time to bring the system to a safe state prior to the attack.

He et al. [6] indicated the benefit of an attacker is based on the loss of defending a system. The damage of defender when the attack action is undetected by the IDS (SD) as:

$$SD = Con_p \times Con_v + Int_p \times Int_v + Ava_p \times Ava_v \quad (7)$$

Con_p,Int_p, Ava_p are the damage degrees the attack action has made on the attack object respectively in Confidentiality, Integrity and Availability. Con_v,Int_v, Ava_v are the objects assets in Confidentiality, Integrity and Availability. These values are not constants, and they can be set by the network administrator.
The damage when the attack is detected (FD) is defined as:

$$FD = (Con_p \times Con_v + Int_p \times Int_v + Ava_p \times Ava_v) - Restore \quad (8)$$

Restore is the recovery on the attack action.

$$Restore = Con_p^r \times Con_v + Int_p^r \times Int_v + Ava_p^r \times Ava_v \quad (9)$$

As with the benefit of attacker, He et al. [6] uses four instances in the case of non-cooperative non-zero-sum static game with complete information, the relations between Strategy Profile and attacker benefit are:

- When the attacker and defender take an action:

$$Benefit\ of\ attacker = (SD) \times (1 - P) + (FD) \times P \quad (10)$$

- When the attacker takes an action and the defender does not:

$$Benefit\ of\ attacker = SD \quad (11)$$

- When the attacker fails take an action and the defender takes an action:

$$Benefit\ of\ attacker = 0 \quad (12)$$

- When the attacker and defender do not take an action:

$$Benefit\ of\ attacker = 0 \quad (13)$$

Plainly stated, the benefit of the attacker is based on the loss of defending the system.

$$Benefit\ of\ attacker = -Benfit\ of\ Defender \quad (14)$$

Cremonini and Nizovtsev [21] defined the benefit of attacker in terms of the amount of effort, measured by time, put by an attacker into an attack. They provide the below calculation.

$$Benefit\ of\ attacker = E\big(B(x)\big) \quad (15)$$

x: The amount of effort placed in the attack.

$$E\big(B(x)\big) = \pi(x) \times G \quad (16)$$

$\pi(x)$: Probability of success of attack given the amount of effort put into attack.
G: One time payoff the attacker receives in the case of successful attack.

4.2 Defender Metrics

In this section we provide insight into the metrics selected involving the cost and benefit from the perspective of the defender.

Cost of Defender. The cost of defender involves the cost of a defender to defend a system against an attack. Below we incorporate literature applying cost of defense.

He et al. [6] indicated the cost of a defender consists of Operational Cost, Response Cost and Response Negative.

- **Operational Cost (OC):** Can be derived from the risk assessment knowledge library.
- **Response Negative Cost (RNC):** Can be derived using the following formula:

$$RNC = -P_a \times Ava_v \tag{17}$$

P_a is in [0, 1] being the damage degree to the availability of the system caused by response actions.

- **Response Cost** (**RC**): Involves the values derived from the Attack-defense Knowledge Library.

He et al. [6] also provided four instances in relation between the Strategy Profile and defender costs in the case of non-cooperative non-zero-sum static game with complete information, which are:

- When the attacker and defender take an action:

$$Cost\ of\ defender = -(RC + P_a \times Ava) \times P \tag{18}$$

- When the attacker takes an action and the defender decides to not defend:

$$Cost\ of\ defender = 0 \tag{19}$$

- When the attacker doesn't take any action and the defender takes an action:

$$Cost\ of\ defender = -(RC + P_a \times Ava) \times P_m \tag{20}$$

- When the attacker doesn't take any action nor the defender:

$$Cost\ of\ defender = 0 \tag{21}$$

P_m: False detection rate of the IDS.

You and Shiyong [22] provided metrics that help compute the cost and payoff of an attacker and defender. Using the performance metrics of exposure factor and average rate of occurrence, we compute single loss expectancy and annual loss expectancy.

- **Single Loss Expectancy (SLE):** Involves the dollar amount associated to a single asset, which is computed using the Asset Value (dollar amount assigned by the network administrator) and the exposure factor (retrieved from a performance metric).

$$SLE = Asset\ Value \times Exposure\ Factor \tag{22}$$

- **Annual Loss Expectancy (ALE):** Involves the dollar amount or time associated to an asset over a particular period of time. The single loss expectancy used above and average rate of occurrence (retrieved from a performance metric) to compute ALE.

$$ALE = SLE \times ARO \tag{23}$$

Benefit of Defender. Benefit of defender involves the benefit of a defender to defend a system against an attack, either prior to or following an attack. Below we provide research assessing benefit of defense.

- **Recovery by Restore (RBR):** Involves the ability for the defender to recover a target system to its original state from an attack action.
- **Resources used by the attacker (RUBA):** Involves quantitatively reflecting the number of nodes used by the attacker, which is m.

$$(RUBA) = m \tag{24}$$

He, et al. [6] defined the benefit of a defender based on damage of defender when attack is successful (SD), damage of defender when attack is detected (FD) and Restore, as explained in the previous section of Benefit of Attacker.

In the case of non-cooperative non-zero-sum static game with complete information, He, et al. [6] uses four instances to describe the relations between Strategy Profile and defender benefit as:

- The attacker and defender both take actions:

$$Benefit\ of\ defender = (SD)\times(1-P) + (FD)\times P \tag{25}$$

- When the attacker takes an action and the defender does not:

$$Benefit\ of\ defender = -(SD) \tag{26}$$

- The attacker does not take an action and the defender takes an action:

$$Benefit\ of\ defender = 0 \tag{27}$$

- When the attacker and defender do not take an action:

$$Benefit\ of\ attacker = 0 \tag{28}$$

- **Loss When Attack is Successful (LWAS):** Involves the degree of damage in which the attacker is able to cause on the target system. This metric is a negative benefit to the attacker, capturing the historical data to improve a defender's incentive to defend.
- **Loss When Attack is Detected (LWAD):** Involves the ability for the defender to recover a target system to a non-compromising state from an attack action. This metric is a positive benefit to the attacker, capturing the historical data to improve a defender's incentive to defend.

4.3 Performance Metrics

Performance metrics entail the assessment of the system performance and evaluation of unlike game theoretic defense models. Typically, the payoff metrics in game models are used to gauge the cost-benefit analysis between the attacker and defender. This alone is not sufficient to measure and validate a particular game model. Therefore, the attacker and defender metrics represent the game, whereas the additional metrics provided under the performance classification represent asset performance towards selecting the best competing game models for defense. The premise involving the performance metrics gives further insight into the knowledge of the attack relative to the asset.

Performance metrics use cost-benefit assessment of attack and defense, risk assessment, and a game theoretic approach to construct an assessment of performance. This will support a network administrator view appropriate metrics when analyzing and selecting a particular game theoretic defense model. Initially the performance metrics are computed using the attack information received, then updated with each attack instance using ADAPT and the defending system. For instance, items such as, false positive (FP) or mean time to incident discovery (MTTID) are set to zero, once computed by the initial attack, these values are updated to provide asset performance relative to the game models. This performance assessment relative to game models provides contribution to existing taxonomies.

In this section we list various performance metrics from literature that can be applied to game theoretic defense models and used for model assessment.

- **Number of rounds to reach Nash Equilibrium (NORRE):** Burke [23] proposed a metric which provides the number of rounds to reach a Nash Equilibrium, in order to evaluate a game theory model of information warfare, based upon the repeated games of incomplete information model. Burke [23] stated equilibrium provides the ability to analyze a game theory model's predictive power, which is evaluated in terms of accuracy and performance.

$$NORRE = Count(actions\ played\ until\ nash\ equilibrium) - 1 \tag{29}$$

- **Overall Game Quality (OGQ):** Jansen [24] stated qualitative assignments can be used to represent quantitative measures of security properties (e.g., vulnerabilities found). We define a metric overall game quality, where the game model is determined based on the availability of the system (e.g. percentage of available bandwidth), the performance of the game (e.g. average NORRE), and the quality of the system (e.g. false positive rate). This metric is based on the overall equipment effectiveness, where game theory parameters are applied to measure the efficiency of various games [25]. Other works utilized false positive rate as a part the actual game model [26]. This metric is resilient to both options of the false positive rate when determining the overall game quality.

$$OGQ = Availability \times Performance \times Quality \tag{30}$$

- **Exposure Factor (EF):** Exposure factor represents the percentage of loss a threat may have on a particular asset. Exposure factor with a combination of other metrics will provide insight to the level of importance a system may have in the event of an attack.

$$EF = \frac{Asset\ Loss}{Tot.Asset\ Level} \tag{31}$$

- **Average Rate of Occurrence (ARO):** Average Rate of Occurrence is an estimate of the frequency of attack probability. Average Rate of Occurrence can assist with determining defense strategies of a specific asset. Minimizing the ARO provides insight to how well a game theoretic defense solution is performing.

$$ARO = \frac{Count\ (Occurrences)}{Time\ Interval} \tag{32}$$

- **Loss of Availability (LOA):** Loss of availability refers to the loss of resource which is currently unavailable to the legitimate requesting processes. The higher the value of this metric incurs an increased loss.

$$LOA = \frac{Count\ (Unavailable\ Resources)}{Tot.No.of\ Legitimate\ Requesting\ Processes} \tag{33}$$

- **Incident Rate (IR):** Incident Rate indicates the number of detected security breaches a system or asset experienced during an allotted time period. Using incident rate, with a combination of other metrics, can indicate the level of threats, effectiveness of security controls, or attack detection capabilities [27].

$$IR = Count(Incidents) \tag{34}$$

- **Mean Time to Incident Discovery (MTTID):** Mean-Time-To-Incident-Discovery characterizes the efficiency of detecting attacks, by computing the average elapsed time between the initial occurrence of an incident and its subsequent discovery. The MTTID metric also serves as a leading indicator of flexibility in system or administrator's ability to defend as it measures detection of attacks from known and unknown vectors [27].

$$MTTID = \frac{Date_{of_{Discovery}} - Date_{of_{Occurrence}}}{Count(Incidents)} \tag{35}$$

- **Mean Time to Incident Recovery (MTTIR):** Mean Time to Incident Recovery measures the effectiveness of recovering from an attack. The more responsive a system or administrator is, the less impact the attack may have on the asset [27].

$$MTTIR = \frac{Date_{of_{Recovery}} - Date_{of_{Occurrence}}}{Count(Incidents)} \tag{36}$$

- **Mean Time to Mitigate Vulnerability (MTTMV):** Mean time to mitigate vulnerabilities measures the average time exhibited to mitigate identified vulnerabilities in a particular asset. This metric indicates a system or administrator's ability to patch and/or mitigate a known vulnerability to reduce exploitation risk [27].

$$MTTMV = \frac{Date_{of_{Mitigation}} - Date_{of_{Detection}}}{Count(Mitigated_{Vulnerabilities})} \tag{37}$$

- **False Negative Rate (FNR):** The frequency in which the system fails to report malicious activity occurs. It involves the number of incidents that are not detected, which are present within the system [28].

$$FNR = \frac{(Missed\ Incidents)}{Count(Incidents)} \tag{38}$$

- **False Positive Rate (FPR):** The frequency in which the system reports a malicious activity in error. It involves the number of incidents that were detected and upon further discovery produced a false incident [10].

$$FPR = \frac{(False\ Positives)}{Count(Incidents)} \tag{39}$$

5 A GAME MODEL COMPARING SYSTEM BASED ON ADAPT

In this section we describe the process in which ADAPT will be used to compare game models followed by a scenario of its application using a distributed denial of service (DDoS) attack. Lastly, we highlight ADAPT's application to the Game Inspired Defense Architecture (GIDA), wherein a game decision system (GDS) uses ADAPT to compare competing game models. The GDS facilitates selecting the optimal game theoretic defense model.

5.1 Methodology

In this section we present the method to compare the candidate game models relevant to an identified attack using metrics in ADAPT. The identified attack is resolved into attack vectors, which is used to locate the relevant metrics within ADAPT. Using these metrics the game models are compared to select the game model most suitable for defense.

In a given attack scenario a certain set of anomalies are identified. Those anomalies are used to identify the attack using the AVOIDIT taxonomy proposed in Simmons, et al. [29]. This identified attack is resolved into "attack components". These attack components are parameters indicating some aspect of the system, albeit malfunction and/or failure, affected by the attack. They are composed of various anomalies which are observed by sensors such as Firewalls, IDS, and their values indicate their severity. Using these attack components a set of metrics that fittingly quantize the system's current security state are identified in ADAPT. Using these metrics the game models with their respective game model components which correspond to these metrics in their interaction modeling in terms of actions-payoff of players are selected. These models are compared with each other to pick the one, which corresponds/maps best to the selected metrics.

The present experiment had a simple case. To achieve the above flow we used the following 5 steps.

1. Given an attack, A, and a target system T, we identify a set of attack components AC.
2. We map the attack components AC_n with its respective ADAPT metric, AM_n.
3. Given the game model and the game model components we provide the Boolean value (0 or 1) to all the metrics. If a game model component corresponds to a selected metric then the component gets a value 1 else a 0. This is done for all the game model components of each of the competing game models.
4. All values associated with each game model component of a game model are summed to give a total score of evaluation of the competing game models.
5. The game model with the highest score is selected as being the most relevant for defense, which is appropriate for instantiation.

In a given model, temporal consideration is not parameterized separately. In terms of actions at a given state of the game and how and when the game transits between the states is considered as the mode to keep track of the time. For more complex scenarios time must be taken into consideration in more explicit ways in the modeling. In the future work we intend to exhibit temporal considerations and improve the evaluation based on weighted values and not just 0/1 for greater precision.

The ADAPT taxonomy is constructed in a way to evaluate the holistic view of a game model, along with its respective system. It requires some resources to instantiate each game model to run a game. The metrics in the performance branch evaluate the overhead of instantiating a game model. The attacker/defender branch metrics evaluate the parameters which affect the attacker/defender payoff. The next section illustrates the ADAPT methodology using a zero-sum game scenario where the game model components correspond to a benefit to the defender, thus correspond to the cost of the attacker and vice versa. Due to space constrains, the reader is encouraged to refer to Bedi, et al. [30] for an elaborate discussion.

5.2 A Case Study: DDoS Attack Scenario

We continue our example from section 2, wherein we analyze a DDoS attack and ADAPT's applicability to discern the main features of the attack. This offers the framework for game model selection with a relevant set of metrics. We focus on the bandwidth reduction where multiple attacking nodes attempt to push their packets to exhaust limited bandwidth of a link in the network. The attacker's strategy is to maximize either the botnet size or the sending rate to flood the pipe. We will call this strategy a flood strategy by the attacker, as he is not concerned with detection, but to overwhelm its target. Whereas the defender's strategy is to implement the optimal firewall setting which will allow legitimate flows and block malicious flows. This defense strategy is simply to defend or not defend.

Experiential knowledge is used to evaluate the crucial features of our DDoS attack example to capture the appropriate attack components for analysis. We illustrate these components with an example. This example is based on prior work in this domain [31, 32].

Attack Components

In our example scenario, the attack is a network based DDoS and it consists of the following attack components:

- v_b: Average bandwidth used by the attacker,
- v_n: Ratio of the number of lost legitimate users to the total number of legitimate users,
- v_c: Number of nodes used by the attacker to launch an attack

The values of these components define the impact of the attack over a target system. In this example, the attacker's goal is to increase v_b and v_n, which are the rewards. An assumption is made on the attacker's cost v_c is linearly proportional to the number of attacking nodes employed and $v_c = m$.

Continuing our DDoS example, the IDS captures a fixed number of properties to begin facilitating situational analysis for decision making, whereas the firewall has a default drop threshold set. Various sources provide input properties used by ADAPT. It is assumed the mapping is preset, which is initially performed manually via expert knowledge and keywords. The initial input properties to ADAPT for the DDoS example are: (a) total bit rate, (b) total number of flows, (c) drop rate, and (d) number of flows dropped.

A legitimate flow is one in which the network bandwidth is used in a fair manner, being the flow per node being less than or equal to the ratio of total bandwidth to the number of nodes. The loss of legitimate flows is used in this example to determine if the flow is negatively impacted. This provides a way to distinguish attacker flows.

The bitrates sum is computed per IP address. The IPs which consume above the amount of bandwidth than their predefined share are considered malicious nodes. For example, for the attacker to break the initial threshold set by the defender there must be a minimum number of unfriendly nodes required to drop at least one friendly (legitimate) node. If the defender initiates a response to the attack, an incurred cost to the defender, is accounted in terms of resources and time.

Similarly, the following attack components, which are used in our example, are mapped to corresponding attacker, defender, and performance metrics.

The first component v_b, being the average bandwidth used by the attacker maps to the following metrics:

(a) The **SLE** metric in ADAPT is classified under the cost of defender. It captures the dollar amount associated to a single asset, which is computed using the Asset value and the Exposure factor. In our scenario, the asset is the bandwidth of the pipe and its value can be determined by the network administrator. We associate the Exposure Factor as the ability of the attacker to access and exploit the asset.
(b) The **EIBA** metric in ADAPT is classified under the benefit of attacker. In our DDoS example, this is associated to the zero-sum game to express the attacker's monetary success.
(c) The **EF** metric in ADAPT is classified under performance. In our example, this metrics is associated with the percentage of loss on the bandwidth.

The second component v_c, being the number of nodes used by the attacker to launch an attack maps the following metrics:

(a) The **RNC** metric in ADAPT is classified under the cost of defender. In our example, this metric is associated with the damage the attack was able to accomplish considering the defender's response.
(b) The **DOA** metric in ADAPT is classified under the benefit of attacker. It involves the monetary value received by the attacker when an attack is successful
(c) The **LOA** metric in ADAPT is classified under performance. It represents the percentage of loss a threat may have on a particular asset.

The third component v_n, being the ratio of the number of lost legitimate users to the total number of legitimate users maps to the following metrics:

(a) The **RUBA** metric in ADAPT is classified under the cost of defender. It relates to quantitatively reflecting the number of nodes used by the attacker
(b) The **COLA** metric in ADAPT is classified under the benefit of attacker. It involves the cost incurred by the attacker when an attack is launched.
(c) The **IR** metric in ADAPT is classified under performance. It represents the incident rate associated to the target system.

Table 1 highlights a visual representation of the attack components we use to map metrics with ADAPT. The column titled "ADAPT Metrics" contain the metrics mapped using the attacker, defender, and performance classifiers. Each component gets mapped to either cost or benefit (but not both) for each of the players; attacker and defender. Also, a component corresponding to the cost (or benefit) of a defender cannot correspond to the cost (or benefit) of the attacker.

Table 1. Attack Components Correlation with ADAPT Metrics

DDoS Attack Components	**ADAPT Metrics**				
	Defender		**Attacker**		**Performance**
	Cost	**Benefit**	**Cost**	**Benefit**	
v_b	SLE	X	X	EIBA	EF
v_n	RNC	X	X	DOA	LOA
v_c	X	RUBA	COLA	X	IR

Table 1 illustrates the ADAPT metrics, which depicts the player and performance related metrics for mapping. Using the described game scenario the defender is able to use ADAPT to systematically retrieve potential game models suitable for defense based on the attack components received and its metric mapping. The scenario has to be evaluated with respect to these three factors, which the metrics in ADAPT capture. Once this is done a relationship between the quantified components of the game governing equations as discussed in the example are evaluated. This makes the game model involving the obtained attack components best depicting the scenario, will be chosen to be the game model that best suits the present scenario. The metrics in ADAPT quantifies the parameters of the scenario. Using these values, the correlation of a model can be evaluated using a suitable algorithm as described in Bedi, et al [30]. As with any sensor, there are instances where false positives occur, in which human intervention is required for the improvement of those sensors. For the purpose of this paper, we assume the attack has a relevant game model in the repository, where human intervention and expert knowledge is required to update the repository for increased accuracy of an ADAPT based system. In future work, we are developing a frame work for constructing game models, which facilitate dynamic analyses of imperfect information and respond with changes in the strategies dynamically for optimum response in real world scenarios. This future work is based on our prior work [26] where we recommend game theoretic defense strategies to network security problems assuming imperfect sensory information.

In our example the strategy of the attacker and defender does not change. For the sake of discussion, let us consider an instance in which the strategy of the attacker changes, by increasing or decreasing the number of nodes exhibited in the DDoS attack. Also, let us consider, the defender is able to change its strategy, as well. In both cases, of the attacker and defender, ADAPT is resilient to the change, as the generalized metrics remain mapped within the taxonomy. Paruchuri, et al. [30] proposed an efficient heuristic approach for security against multiple adversaries where the attacker is unknown to the defender. This work is in line with our DDoS example, due to its unknown nature of the true attacker.

5.3 ADAPT in the Game Inspired Defense Architecture

The Game Inspired Defense Architecture (GIDA) is foreseen as a holistic approach designed to counter cyber-attacks [26, 30, 34, 35]. GIDA (Figure 2) focuses on the concept of offering defense strategies against probable and committed attacks by modeling situations as multi-player game scenarios. The attack-defense analysis is done by ADAPT. GIDA provides security by operating in the following fashion: Identification of attack, Extraction of game models relevant to the identified attack, and Assessment of candidate game models and execution of the one which is most relevant to present attack.

GIDA consists of three components, namely, ADAPT (our taxonomy), a Knowledge Base (KB), and a Game Decision System (GDS). The GDS is a preventative system, within the GIDA framework, to collect input from various sources for continuous attack information updates relative to game models.

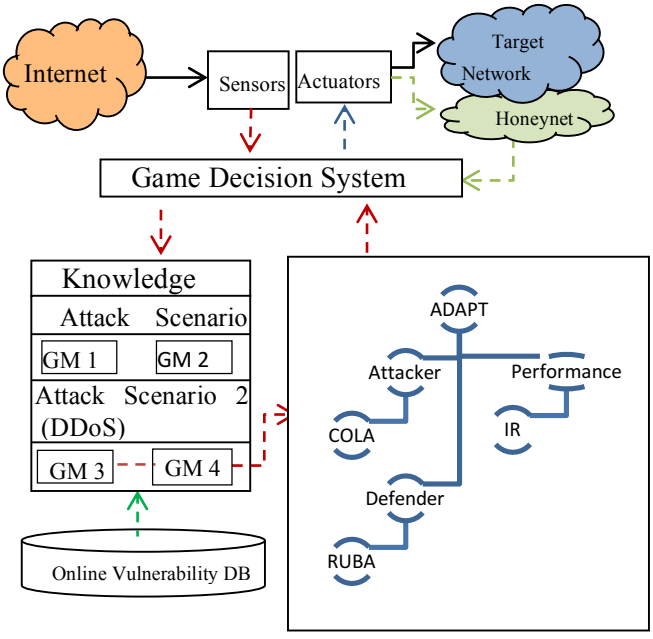

Fig. 2. Game Inspired Defense Architecture

The knowledge base (KB) consists of game models mapped to the types of attacks identified and additional attack related data. The GDS operates in a preventative fashion through the assessment of candidate game models respective to a particular attack and executes the game model which is best among them. ADAPT provides the metrics to be mapped to the components, and evaluate them in terms of different aspects of the player's payoffs, and the game's performance. This gives the GDS the specific set of game metrics defining the ongoing attack. The GDS acts as the brain with provisions to process input information and take the appropriate action.

One implementation of our proposed defense architecture is depicted (Figure 2). Our network topology consists of a Target Network which our architecture aims to protect. This network is connected to the Internet through a series of Sensors and Actuators. Currently, GIDA uses an intrusion detection system (IDS) as the sensor and a firewall as the actuator. The topology also includes a honeynet, which is a network of honeypots. The honeypot is primarily used as a virtual implementation of the target network for analyzing traffic and gathering additional information from the attacker.

Once an attack is identified against a target, the sensors feed information to the GDS. The GDS contains an attack identification mechanism, which forwards the suspected attack to the KB. The KB is searched for additional attack related information and candidate game models which can defend against the identified attack. In this present case (Figure 2), the knowledge base provides two game models: GM 3 and GM 4. These suggested game models are then sent to ADAPT to assess the attack, defender, and performance metrics for selection of the optimal game model.

The depiction of ADAPT (Figure 2) highlights how ADAPT uses its knowledge of the two game models to classify each component of an attack with the game metrics. Due to space constraints, we provide a single example of a component's selection process using the tree structure of ADAPT (Figure 2). ADAPT navigates its tree for each component of the attack to capture the metrics from the identified attack for analysis. These metrics are used to evaluate the computed cumulative score of the selected game models. The GDS uses ADAPT to select the model which possesses greater relevance to the present observed attack based on each attack components impact to the attacker, defender, and the performance of the system during the game. Once a game model is selected, the GDS executes the game model by sending the proposed defense actions to the respective sensor or actuator. Updated information is obtained via the KB's ability to access vulnerability databases such as National Vulnerability Database (NVD), MITRE Corporation's Common Vulnerabilities and Exposures (CVE) list, etc.

We envision this process of attack identification and defense to be iterative in nature where sensors like IDS constantly provide input to GIDA. Based on these inputs, the GDS, ADAPT, and the KB reevaluates their findings to further improve the proposed defense measures. This process continues until the attack is subdued. It should be noted that GIDA has an option of playing a selected game. Simple games such as firewall setting changes may be performed automatically, however defender interaction may be required for complex games. Nagaraja and Anderson [36] provided insight into discovering the effectiveness of iterated attack and defense operations through a proposed framework using evolutionary game theory.

Moreover, there are various types of plausible attacks on any given target system. GIDA uses the GDS to address attacks before they reach fruition to observe and attempt to make a decision on the optimal game model for defense. This gives GDS the ability to operate in a reactive manner, as well, considering attacker initiates. We anticipate certain attacks to be continuous in nature and the intention is to impede any or further damage to its respective target, hence the GIDA framework is proactive to prevent damage on a monitored network.

6 RELATED WORK

There are several recent efforts which consider security games evaluation, involving performance and security metrics. In this section we provide an overview of literature relative to game theory defense models and performance metrics.

He, et al. [6] proposed a novel Game Theoretical Attack-Defense Model (GTADM) which quantifies the probability of threats in order to construct a risk assessment framework. They focus on the computation of the attack probability according to the cost-benefit of the attacker and the defender, and defined relevant metrics to quantify the payoff matrix.

Alpcan and Basar [25] proposed a game theoretic analysis of intrusion detection in an access control environment. They provided several common metrics that were used to help identify the performance of the Intrusion Detection System IDS. Using the metrics they provided, simulation was used to determine the costs and actions of the attacker and IDS.

Bloem, et al. [37] proposed an intrusion response as a resource allocation problem, where the resources being used were the IDS and network administrator. They provided insightful metrics regarding the response time of an IDS and its ability to respond without the administrator's involvement. Also, they used an administrator response time metric to determine the time of effort used to compute administrator involvement after an alert from the IDS. This metric can prove beneficial in determining how well a system is able to successfully respond against attacks while minimizing the administrator's involvement.

Liu, et al. [38] proposed an incentive based modeling and inference of attacker intent, objectives, and strategies. They provided several examples that compute the bandwidth before, during, and after an attack. They specified metrics to compute the

absolute impact and relative availability to determine the system degradation. These metrics are used to distinguish how well the system was able to capitalize on the attack, as well as how well the attacker was able to succeed in reducing the bandwidth.

You and Shiyoung [22] proposed a network security behavior model based on game theory. They provide a framework for assessing security using the Nash equilibrium. In assessing the security, they also provide metrics used to analyze the payoff and cost of an attacker and defender using the exposure factor, average rate of occurrence, single loss expectancy, and annual loss expectancy.

Savola [8] surveyed emerging security metrics approaches in various organizations and provided a taxonomy of metrics as applicable to information security. His taxonomy provided a high level approach to classifying security metrics for security management involving organization, operational, and technical aspects. He also included high level classification for metrics involving security, dependability, and trust for products, systems, and services. The metrics provided are all high level, with a lack of specific metrics used for each category, but he provides a good starting point to organizations needing to begin analyzing various security metrics within their organization.

Fink et al. [39] proposed a metrics-based approach to IDS evaluation for distributed real-time systems. They provided a set of metrics to aid administrators of distributed real-time systems to select the best IDS system for their particular organization. They presented valuable information needed to gather the requirements of an organization in order to capture the importance, and use the requirements to successfully measure the performance according to requirements imposed by the organization.

7 CONCLUSION AND FUTURE WORK

Game theoretic models continue to present information and analysis to initiate defense solutions against an attack for a network administrator. This paper is an attempt to provide an intuitive game theoretic metric taxonomy that a defender can use to synthesize how well a particular game model is performing in a network. We assume the collected metrics are generic and can be used regardless of the type of game theoretic model used for defense. We believe providing a list of metrics for a game inspired defense architecture will provide an administrator with the appropriate information to make an intelligent decision in game theoretic defense analysis. This assumption is not approved through real experiences.

Creative metrics are necessary to enhance a network administrator's ability to compare various defense schemes. We propose a game theory inspired Attack-Defense And Performance metric Taxonomy (ADAPT) to help a network administrator view pertinent metrics during a game theoretic model analysis. Although this work provides game related model selection, alternative solutions of ADAPT can be used without a game theoretic aspect.

Future work involves demonstrating the usefulness of ADAPT through the implementation of the game decision system (GDS), which assists a game inspired defense architecture with model selection. We are currently in progress towards developing the game decision system based on ADAPT using an open source knowledge base to store metrics associated to particular attack and game models. The game strategies will be assessed using a weighted score ranking between models which will assist with selecting the game with the most relevance to the identified attack. The use of ADAPT in this system will have knowledge of the attack and its target to assess the proposed game decision strategies to defend against the attack. In the event an attack is not mapped, we will construct game models to handle such scenarios. We intend to implement the model described within He, et al. [6], as well as others, to compare results with an ADAPT based system. Furthermore, an enhancement to the taxonomy may be considered with an additional game theoretic defense model classification distinguishing the various game models. We foresee using an ADAPT based system as a comprehensive solution to optimal game selection.

8 REFERENCES

1. Hamilton, S. N., Miller, W. L., Ott, A. and Saydjari, O. S. "The role of game theory in information warfare," Proceedings of the 4th information survivability workshop (ISW-2001/2002), 2002.
2. Jiang, W., Tian, Z., Zhang, H., and Song, X. "A Stochastic Game Theoretic Approach to Attack Prediction and Optimal Active Defense Strategy Decision," In IEEE International Conference on Networking, Sensing and Control, pages 648 –653, April 2008.
3. Bellovin, S., "On the Brittleness of Software and the Infeasibility of Security Metrics," *IEEE Security and Privacy*, Volume 4, Issue 4, July-Aug. 2006.
4. National Cyber Security Research and Development Challenges Related to Economics, Physical Infrastructure and Human Behavior: An Industry, Academic and Government Perspective, The Institute for Information Infrastructure Protection (I3P), 2009, http://www.thei3p.org/docs/publications/i3pnationalcybersecurity.pdf.
5. Gopalakrishnan, J., Marden, R., and Wierman, A. "An architectural view of game theoretic control", *ACM SIGMETRICS Performance Evaluation Review*, Volume 38, Number 3, 2011.

6. He, W. and Xia, C. and Wang, H. and Zhang, C. and Ji, Y., "A Game Theoretical Attack-Defense Model Oriented to Network Security Risk Assessment", Proceedings of the 2008 International Conference on Computer Science and Software Engineering, vol. 3, 2008.
7. Bryant, A. R. "Developing a framework for evaluating organizational information assurance metrics programs," Thesis, Airforce Institute of Technology, Defense Technical Information Center, 2007.
8. Savola, R., "A Novel Security Metrics Taxonomy for R&D Organizations," Proceedings of the 7th Annual Information Security Conference, 2008.
9. Wesner, J. W., "Winning with quality: Applying quality principles in product development," New York: Addison-Wesley, 1994.
10. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V. Wu, Q., "A Survey of Game Theory as Applied to Network Security," HICSS43 Hawaii International Conference on System Sciences, 2009.
11. Mirkovic, J., and Reiher, P. "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," In ACM CCR (April 2004).
12. Li, Z., Goyal, A., Chen, Y., and Paxson, V. "Automating analysis of large-scale botnet probing events," In ASIACCS '09, 2009.
13. Parameswaran, M., Rui, H., and Sayin, S. "A game theoretic model and empirical analysis of spammer strategies," In Collaboration, Electronic Messaging, AntiAbuse and Spam Conf., number 7, 2010.
14. Payne, S., "A Guide to Security Metrics", SANS Institute, June 2006.
15. Swanson, M. NIST Special Publication 800-55: Security Metrics Guide for Information Technology Systems, 2003.
16. The National Science and Technology Council. Federal plan for cyber security and information assurance research and development, 2006.
17. Vaughn, R., Henning, R., and Siraj, A. "Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy," Proceedings of 36th Hawaii International Conference on System Science (HICSS '03), 2003.
18. Manadhata, J. and Wing, P., "An attack surface metric", Technical Report CMU-CS-05-155 (2005).
19. Carin, L., Cybenko, G., and Hughes, J., "Quantitative Evaluation of Risk for Investment Efficient Strategies in Cyber security: The QuERIES Methodology," *IEEE Computer*, 2008.
20. Lye, K. and Wing, J., "Game strategies in network security," Proceedings of the Foundations of Computer Security, 2002.
21. Cremonini, M. and Nizovtsev, D., "Understanding and Influencing Attackers Decisions: Implications for Security Investment Strategies," 5th Workshop on the Economics of Information Security, June 2006.
22. You, X. and Shiyong, Z.,"A kind of network security behavior model based on game theory," Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003.
23. Burke, D.A., "Towards a game theory model of information warfare," Master Thesis, Air Force Institute of Technology. USA, 1999.
24. Jansen, W., "Directions in Security Metrics Research," NISTIR 7564, March 2009.
25. Alpcan, T. and Baser, T., "A game theoretic analysis of intrusion detection in access control systems," Proc. of the 43rd IEEE Conference on Decision and Control, 2004.
26. Shiva, S., Roy, S., Bedi, H., Dasgupta, D., and Wu, Q. 2010. "An Imperfect Information Stochastic Game Model for Cyber Security," The 5th Intnl Conference on i-Warfare and Security.
27. Center for Internet Security. "The CIS Security Metrics" https://www.cissecurity.org/tools2/metrics/CIS_Security_Metricsv1.0.0.pdf, May 2009.
28. McGraw, G. Software Security: Building Security In. Addison-Wesley, 2006.
29. Simmons, C., Shiva, S., Dasgupta, D., and Wu., Q. "AVOIDIT: A cyber attack taxonomy," Technical Report: CS-09-003, University of Memphis, August 2009.
30. Bedi, H., Shiva, S., Simmons, C., and Shandilya, V. "A Game Inspired Defense Architecture," GameSec 2012 (Poster), Conference on Decision and Game Theory for Security, 2012.
31. Wu, Q., Shiva, S., Roy, S., Ellis, C., and Datla, V. "On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks," SpringSim, 2010.
32. Bedi, H., Roy, S., Shiva, S. "Game Theory-based Defense Mechanisms against DDoS Attacks on TCP/TCP-friendly Flows," IEEE Symposium on Computational Intelligence in Cyber Security, Paris, France, 2011.
33. Paruchuri, P., Pearce, J. P., Tambe, M., Ordonez, F., and Kraus, S. "An Efficient Heuristic Approach for Security Against Multiple Adversaries," In AAMAS, 2007.
34. Shiva, S., Roy, S., Dasgupta, D., "Game Theory for Cyber Security," 6th Cyber Security and Information Intelligence Research Workshop, April 2010.
35. Shiva, S., Bedi, H., Simmons, C., Fisher, M., Dharam, R. "Holistic Game Inspired Defense Architecture," International Conference on Data Engineering and Internet Technology, March, 2011.
36. Nagaraja, S. and Anderson, R. "The topology of covert conflict," in Proceedings of the 5th Workshop on The Economics of Information Security (WEIS 2006), 2006.
37. Bloem, M., Alpcan, T., and Basar, T. "Intrusion response as a resource allocation problem," IEEE Conference on Decision and Control, 2006.
38. Liu, P., Zang, W., and Yu, M., "Incentive-based modeling and inference of attacker intent, objectives, and strategies," ACM Transactions on Information and System Security (TISSEC), 2005.
39. Fink, G., Chappell, B., Turner, T., and O'Donoghue, K., "A metrics-based approach to intrusion detection system evaluation for distributed real-time systems," in Proceedings of the 16th International Parallel and Distributed Processing Symposium, Fort Lauderdale, FL, USA, April 2002.