A Game Inspired Defense Architecture

Harkeerat Bedi, Sajjan Shiva, Chris Simmons, Vivek Shandilya

Department of Computer Science

University of Memphis, TN, U.S.A.

(hsbedi, sshiva, cbsmmons, vshandilya@memphis.edu)

2012 Conference on Decision and Game Theory for Security (GameSec 2012)

Abstract

The effectiveness of game theory in network security is being researched extensively by modeling the attackers and defenders as players interacting in a game.

We propose a preliminary study towards building a *game inspired defense architecture* (GIDA) which aims to provide quantifiable defense mechanisms to real world security problems by modeling them as multi-player games.

We demonstrate the applicability of our defense architecture using a distributed denial of service attack scenario and verify its effectiveness via simulation.

Game Inspired Defense Architecture

Our architecture consists of a Game Decision System and a Game Repository.

The Game Repository is a database populated by security experts and it consists of a mapping between the various kind of attacks and their potential defense game models.

The Game Decision System (GDS) is used to compare potential game models for a particular attack and execute the one which is most relevant. GDS consists of:

1. A taxonomy of game related metrics called Attack-Defense and Performance metric Taxonomy (ADAPT) [1]
2. A Game Assessment Algorithm for comparing potential game models to pick the one which is most beneficial to the defender.

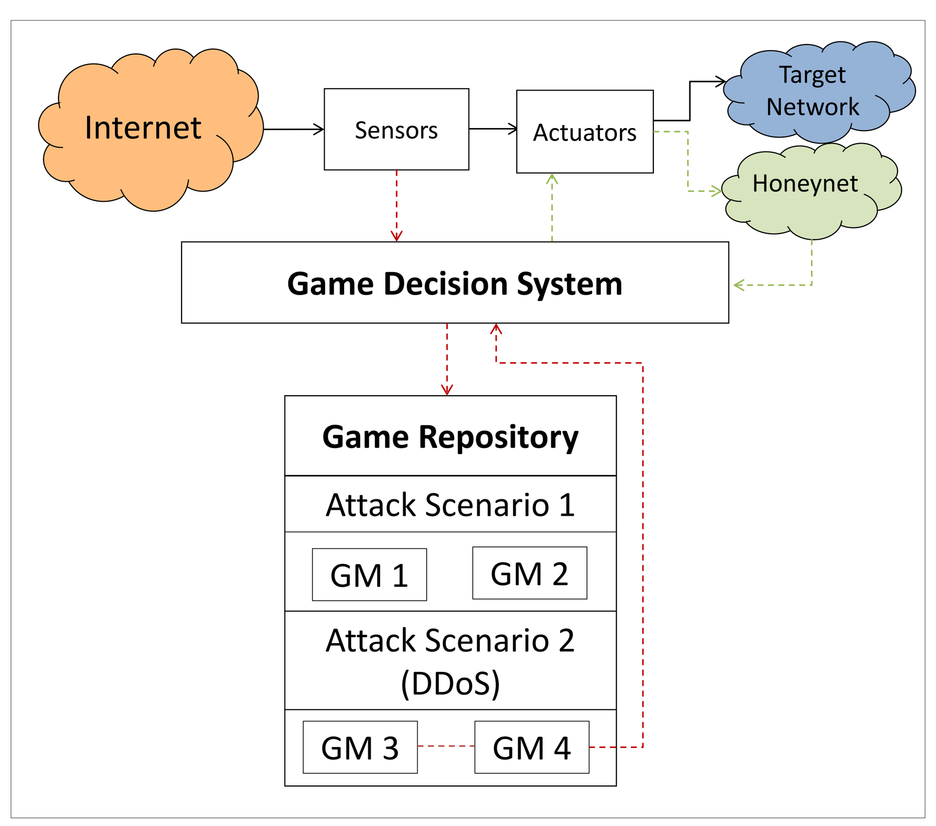

Fig. 1. Game Inspired Defense Architecture

Fig. 1. shows GIDA in operation. The Internet can access the Target Network through a network of Sensors (e.g. IDS, s/w monitors, log parsers), Actuators (e.g. firewalls, routers).

Incoming traffic is first parsed through the Sensors which monitor it for anomalies. Once an attack is identified, the GDS is notified. The GDS queries the Game Repository for potential game models for this particular attack. This this case the attack is a DDoS and the potential game models are GM 3 and 4.

These game models are returned to GDS which uses the Game Assessment Algorithm with ADAPT to identify the best game model for this particular attack. The defense actions are then forwarded to the Actuators, which in this case decided either to drop, redirect to honeypot or allow incoming traffic to the Target Network.

Game Assessment Algorithm

The Game Assessment Algorithm takes game models as its input and uses ADAPT to provide a relevancy score R for each game model. This score is based on the relevance between attack components and game model components.

Attack components represent the different kinds of impact an attack can have on a target system. Game model components correspond to the attack components of the attack they address.

Game model with the highest score is selected and then used by GDS for defense. We explain this algorithm below using a DDoS attack scenario.

Input: A set of game models J, a set of attack components c_A
Output: A game model j best suited for defense

Game Assessment Algorithm

1. **for** each i^{th} attack component c_{A_i}
2. identify its corresponding metrics $c_{A(a,d,p)}$
3. **end for**
4. Initialize the relevance score $R = 0$ for all game models $j \in J$
5. **for** each game model $j \in J$
6. **for** each game model component c_{j_i} in j
7. compute component relevance score R_{j_i} based on $c_{A_{i(a,d,p)}}$
8. **end for**
9. **end for**
10. Add the component relevance score for each game model to R_j
11. Return game model j with the highest relevance score R_j.

Fig. 2. Game Assessment Algorithm

Attack Scenario: Distributed Denial of Service (DDoS)

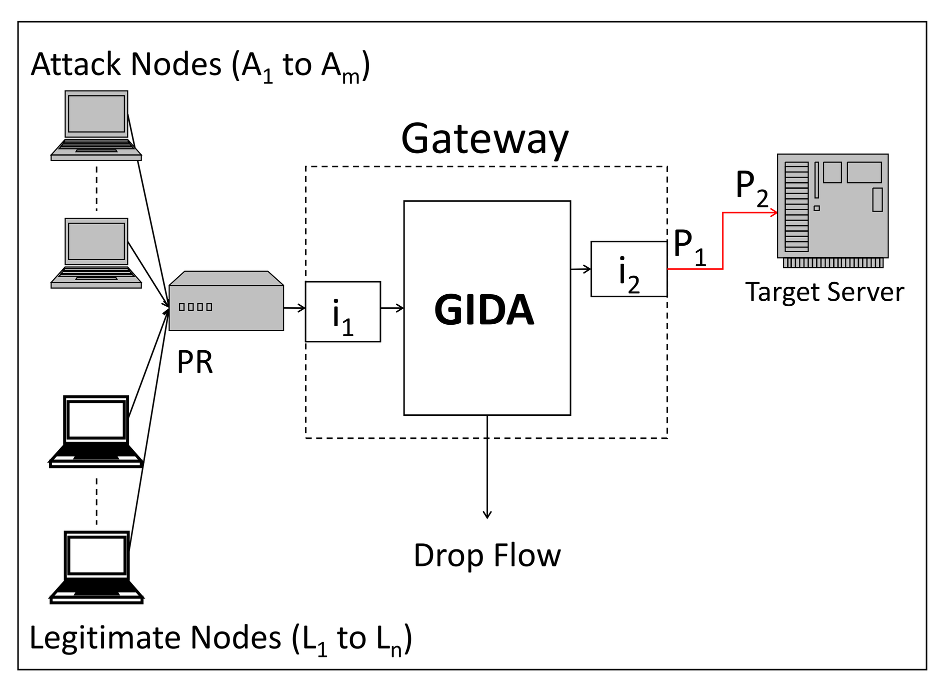

Fig. 3. DDoS Attack Network Topology

We consider a standard DDoS attack scenario which was presented in our earlier work [2] where m attacker nodes are used to send bogus traffic to the Target Server. The bottleneck pipe (P_1, P_2) is prone to congestion when the attacker nodes send more than their fair share of traffic. This eventually causes the n legitimate nodes to lose their fair share of the pipe which results in a denial of service attack.

Here, the attacker's action set includes setting the number of nodes to use, and the amount of traffic to send per node. The defender's (GIDA) action set includes adjusting the firewall to rate-limit the traffic from the attacker nodes.

We define a DDoS attack by the following attack components:

v_b: The attacker's average b/w consumption of $(P_1 - P_2)$.
v_n: The ratio of lost users to the total users on average.
v_c: Number of attack nodes employed.

Game Model Assessment

Game Model 1
This model was proposed in our prior work [2] which defended against the DDoS attack discussed in Section 3.1. It evaluated the attacker and defender's payoffs and proposed a pair of optimal strategies for both players (attacker and defender) by computing a Nash equilibrium (NE). The payoffs of each player are based on the values of the following three game model components:

v_b: The attacker's average bandwidth consumption of the pipe $(P_1 - P_2)$.
v_n: The ratio of lost users to the total number of users on average.
v_c: Number of attack nodes employed.

We model the attacker's net payoff as a weighted sum of the above three quantities defined as: $V^a = w_b^a \cdot v_b + w_n^a \cdot v_n - w_c^a \cdot v_c$. Here w_b^a, w_n^a, and w_c^a are the weights which determine the impact of the each component towards the attacker's payoff.

Game Model 2
Game model 2 is an alternate game model which counters the same DDoS attack as explained earlier. However, in this case, the payoffs of each player are based on values of only the following two individual components instead of three: v_b and v_n.
Thus $V^a = w_b^a \cdot v_b + w_n^a \cdot v_n$.

Game Assessment:
The Game Assessment Algorithm uses the metrics defined in ADAPT taxonomy to compare the relevance between the attack components and game model components. The table 1 shows the correlation between DDoS attack components with ADAPT metrics.

DDoS Attack Components	ADAPT Metrics				
	Defender		Attacker		Performance
	Cost	Benefit	Cost	Benefit	
v_b	Single loss expectancy	X	X	Expected income by the attacker	Exposure factor
v_n	Response negative cost	X	X	Damage of attack	Loss of availability
v_c	X	Resources used by the attacker	Cost of launching an attack	X	Average rate of occurrence

If each node costs $\$x$ to acquire and use, then the attacker has to spend $m \cdot \$x$ in total, where m is # of attacker nodes.

$$(att\_cost) = m \cdot \$x$$

The metric "resources used by the attacker (att_res)" quantitatively reflects the number of nodes used by the attacker, which is m.

$$(att\_res) = m$$

Since the rate of occurrence of the attack is directly proportional to the number of nodes being employed by the attacker, the metric "average rate of occurrence (ARO)" correlates to the component v_c.

$$(ARO) \propto m$$
$$(ARO) = k \cdot m$$

Where k is a constant. Since game model 1 accounts for these metrics by its third component and game model 2 does not, the game model 1 addresses the attack more comprehensively when compared to game model 2.

That is, game model 1 is more relevant to the attack than game model 2 by the value of (att_cost, att_res, ARO).

$$R_1 - R_2 = (att\_cost, att\_res, ARO)$$
$$R_1 - R_2 = (m \cdot x, m, k \cdot m)$$

Thus by using the game model 1, the defender would be able to defend the attack better than when compared to game model 2.

Results: Game Model Evaluation

Fig. 4 shows the NE obtained for our DDoS attack scenario when game model 1, which consists of three components, is used for the computation of the players' payoff values. We notice that the game model converges at Nash equilibrium at a saddle point (190,28,389.9).

Since game model 2 does not consider the component v_c, the attacker's cost of employing nodes is not considered for the NE evaluation. In this case, the game model 2 would suggest the defender the best strategy of setting his firewall threshold to 245 units, as seen in Fig. 5.

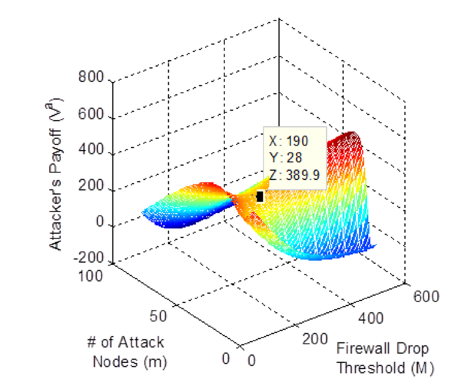

Fig. 4. Nash equilibrium obtained using game model 1 for our DDoS scenario

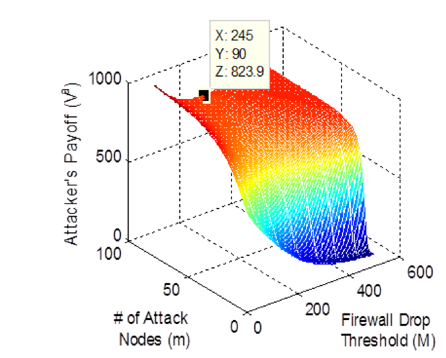

Fig. 5. Nash equilibrium obtained using game model 2 for our DDoS scenario

Fig. 6 shows the payoff obtained by the attacker when the defender plays the strategy (firewall threshold 245) as suggested by game model 2.

We observe, that in this case, the attacker gets a higher payoff (409.1 vs. 389.9), which is worse for the defender.

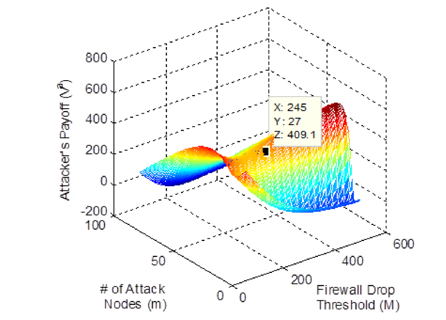

Fig. 6. Payoff (z=409.1) when the defender uses the firewall threshold as 245.

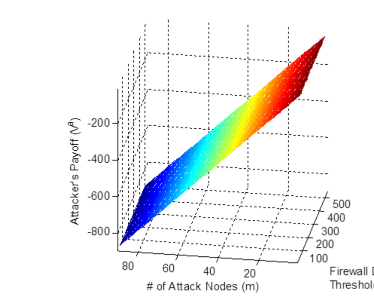

Fig. 7. Potential difference between game model 1 and 2

Thus by using the game model (model 1) suggested by GIDA, the defender achieves a higher payoff.

Fig. 7. highlights the difference in relevance $(R_1 - R_2)$ between game models 1 and 2, which also translates to degree of benefit the defender can obtain, if he chooses the game model 1 for it's defense.

Conclusion and Future work

As cyber attacks become more and more complex, the need for a quantitative and methodological approach towards their mitigation becomes even more important. This poster highlights an ongoing research towards a unique defense architecture (GIDA) which aims to use game theoretic concepts to model and counter cyber-security attacks.

By using a taxonomy of game related metrics along with a game model assessment algorithm, GIDA aims to recommend and execute defense game models which can yield the highest payoff to the defender. Our future work includes working with open source tools like BRO IDS, Click modular router and public testbeds like DETER to extend the applicability of our implementation.

References:
[1] C. Simmons, H. Bedi, S. Shiva, V. Shandilya, "ADAPT: A Game Inspired Attack-Defense And Performance Taxonomy," Technical Report: CS-11-002, University of Memphis, June 2011.
[2] Q. Wu, S. Shiva, S. Roy, C. Ellis, V. Datla, and D. Dasgupta. On Modeling and Simulation of Game Theory-based Defense Mechanisms against DoS and DDoS Attacks. 43rd Annual Simulation Symposium (ANSS10), part of the 2010 Spring Simulation MultiConference, April 11-15, 2010.