OPEN ACCESS

Key Words
Game theory, bayesian game, stochastic game, cybersecurity

Corresponding Author
Rushyanth Narindi,
Gannon University, 109 University Square, Erie, PA 16541, United States

Received: 24 January 2023
Accepted: 2 February 2023
Published: 12 February 2023

Citation: Rushyanth Narindi and Rashid Khan, 2023. Network Security and Privacy Using Game Theory. ACE J. Comput. Sci. Eng., 2: 12-16, doi: 10.59218/makacejcse.2023.12.16

Network Security and Privacy Using Game Theory

Rushyanth Narindi and Rashid Khan
Gannon University, 109 University Square, Erie, PA 16541, United States

ABSTRACT
The topic of network security is challenging and intricate. Researchers have been studying network protection methods for over two decades but the problem of network security remains unresolved. Those who defend against cyber threats face an unfair challenge. They must continuously expand the boundaries of their network defenses to prevent intrusions. Even a small weakness or gap in the system's protections can provide attackers with a pathway through the complex network of defenses.

INTRODUCTION

Information assets are constantly at risk from cyberattacks, occurring as frequently as every 39 seconds, the University of Maryland Clark School of Engineering reported in a survey. These attacks are not politically motivated and cybercriminals target a variety of entities, including large and small businesses, government agencies, non-profit and religious groups, and individuals. To protect their digital assets, organizations are recognizing the importance of investing in skilled personnel and dependable technology safeguards, as the likelihood and impact of cyberattacks continue to rise. The principles of game theory can aid in comprehending any economic, political, or social situation that involves individuals with distinct objectives or preferences, making it a valuable tool for evaluating cyber protection solutions for both technical and non-technical stakeholders.

Game: Game theory is a framework that describes the strategic interaction between parties with opposing or aligned objectives, while considering the possible outcomes and incentives associated with various actions. It involves modeling the decision-making process of individuals or groups as they choose among different strategies based on their beliefs about the actions of others and the payoffs associated with each outcome. The purpose of game theory is to predict the behavior of rational decision-makers in a given situation and to identify optimal strategies for achieving desired outcomes, given the actions of others[1].

Player: In a game, the player assumes the role of a key character who is responsible for choosing actions. This character can be a human, a machine, or a group of individuals.

Action: In this specific game, each action is considered as a move.

Payoff: The advantage or disadvantage given to a player for making a specific move during the game.

Strategy: A gameplay option available to the player during the game.

Strategy: A gameplay option available to the player during the game.

Perfect information game: A perfect information game is a game where all players have complete knowledge of the previous moves made by every player. Examples of perfect information games include go, tic-tac-toe, and chess. On the other hand, a game with incomplete information is a game where at least one player lacks knowledge of one or more of the moves made by another player.

Complete information game: In this game, each player has knowledge of the payoffs and strategies of every other player but not necessarily their specific actions. This term is sometimes used interchangeably with perfect information games but it differs in that it does not take into account the past moves made by players. However, in imperfect information games, at least one player does not know the strategies and outcomes available to the other players.

Bayesian game: A Bayesian game is a type of game in which players are assigned a "type" at the beginning of the game and have imperfect information about the strategies and outcomes of the other players. These games are named after the Bayesian analysis, which is used to predict the outcome of the game.

Static/strategic game: A single-person game where each player chooses their course of action and decisions are made simultaneously by all participants. In this type of game, players are unaware of the choices made by the other players when making their own decision. This is commonly known as a "simultaneous game" or a "static game" throughout the essay[2].

Dynamic/extensive game: A dynamic game is a type of game where players can consider their actions across multiple stages simultaneously. It can be seen as a sequential arrangement of the decision-making problems that players encounter in a static game. A dynamic game may have either finite or endless sequences. This type of game is referred to as a "dynamic game" throughout the rest of the essay.

Stochastic game: A Markov decision process (MDP) is a type of game where players transition probabilistically between different states in the system. The game progresses through a series of states, starting in an initial state where players make decisions and receive rewards based on the current state of the game. The events in a dynamic game might be either limited or infinite.

MATERIALS AND METHODS

Game theory suggests that each "game" involves two or more rational players who select strategies that maximize their expected rewards from participating in the game. In the context of cyber security, a "player" can be a group of individuals working together to achieve a common objective. For example, in a hypothetical game, Player 1 could represent a team of cyber security experts from a reputable company (Company X) responsible for safeguarding the company's information assets, while Player 2 could represent a criminal organization attempting to compromise those same assets.

RESULTS AND DISCUSSION

To represent this game, we can use a simple matrix with rows for Player 1's strategies and columns for Player 2's strategies. The payoffs (E) are displayed at the intersection of each player's strategy, as shown in Table 1, with Player 1's value on the left and Player 2's value on the right:

In the hypothetical game, each player has two possible strategies. Team Defense must decide between implementing Strategy A, which involves creating a security control to protect an information asset, or accepting the risk of an unmitigated attack (Strategy B). Team Offense, on the other hand, must choose between targeting the same asset (Strategy C) or ignoring it (Strategy D).

For the purpose of this example game, let's assume that Team Defense's decision to defend the asset is effective and that Team Offense is successful in their attack on an undefended asset.

Based on the game scenario, we can make predictions about the various trade-offs that each player will consider when deciding on their strategy. We can summarize the factors that Team Defense will take into account while determining its approach as follows:

- The asset's value to the company
- Increasing and sustaining customer confidence
- Complying with laws and regulations
- Materials needed for execution and upkeep
- Usefulness (convenience for genuine consumers in getting their jobs done)

Similarly, we may list some of the elements Team Offense will take into account while determining its plan of action:

- The asset's value if it is jeopardized
- Materials needed to carry out an assault
- Planning and carrying out an attack call for expertise abilities
- The need to protect their proprietary exploits (TTP)
- Chance of being observed (fines, lawful actions, etc.)

Understanding the payoffs for each player is crucial in analyzing a game and making strategic decisions. In our scenario game, the payoffs are displayed in the matrix (Table 2), where the numbers represent the rewards that each player would receive depending on the combination of strategies they choose. By analyzing the payoffs, we can determine the best course of action for each player, taking into account the actions of the other player. However, it is important to note that in real-life cyber warfare scenarios, the payoffs and strategies may be much more complex and difficult to predict, making it challenging to apply game theory concepts.

Table 1: Payoffs (E) player strategy with player 1's and 2's value

		Team offense	
		Strategy C	Strategy D
Team deffense	Strategy A	E1, E2	E1, E2
	Strategy B	E1, E2	E1, E2

Table 2: Payoffs matrix

		Team offense	
		Attack	Don’t attack
Team deffense	Defend	50,-5	25,0
	Don’t defend	-100,25	50,0

The outcome of the (Attack, Defend) game is actually morefavorable for Defense Team, as they were able to successfully defend their asset and gain 50 points, while Offense Team lost 5 points due to their unsuccessful attack. This outcome is in line with the values and goals of each team, as Team Defense wants to protect their assets and minimize the risk of a security breach, while Team Offense wants to gain access to those assets and maximize their potential gains. Team Defense's Worse Scenario Case for Team Defense would be if they choose to not defend their asset (strategy B) and Team Offense chooses to attack (strategy C), resulting in a successful breach and a loss of 100 points for Team Defense.

In our hypothetical game, the payouts for Team Defense in the (Defend, Don't Attack) game are 25, while Team Offense receives no points. In this game, Team Defense implements a security measure to protect an asset, while Team Offense decides not to attack it. Although the security measure may make it more difficult for authorized users to access the asset, it does satisfy one or more compliance criteria. The (Defend, Don't Attack) strategy doesn't benefit Team Offense but it also doesn't cost them anything. The worst outcome for Team Defense is the (Don't Defend, Attack) game, where they don't implement a security measure, allowing Team Offense to successfully breach the asset and resulting in a payoff of -100 for Team Defense. The best outcome for Team Offense is the (Don't Defend, Attack) game, where they successfully breach the asset without encountering any security measures and gain a payoff of 25.

In the game "Don't Defend, Don't Attack", Team Defense chooses not to implement any security measures to protect the asset, and Team Offense decides not to attack it. Team Defense is rewarded with 50 points for their decision not to use resources and interfere with the normal business operations of

Table 3: Best strategies matrix

		Team offense	
		Attack	Don't attack
Team deffense	Defend	50, -5	25, 0
	Don't defend	-100, 25	50, 0

Table 4: Optimal strategies for each player that maximize their individual payoffs

Solve for p	Solve for q
$E_{offense}$ (Defend) = $E_{offense}$ (don't defend)	$E_{offense}$ (attack) = $E_{offense}$ (Don't attack)
-5p+(1-p)25 = 0	-5q + (1-q)25 = 0
-5p+25-25p=0	-5q+25-25q = 0
30p=25	30q = 25
p = 5/6	q = 5/6

Table 5: Anticipated payoffs for each player based on the probabilities

		Team offense	
		Attack	Don't attack
Team deffense	Defend	5/6*1/7=5/42	5/6*6/7= 30/42
	Don't defend	1/6*1/7=1/42	1/6*1/7 = 6/42

Table 6: expected rewards for each participant, assuming they decide to participate in the game

Expected payoff for team defense	Expected payoff for team offense
$E_{DEFENSE}$ = (5/42)*50 +(30/42)*25+(1/42)*-100+(6/42)*50	$E_{OFFENSE}$ = (5/42)*-5+(30/42)*0+(1/42)*25+(6/42)*0
$E_{DEFENSE}$ = 5.95+17.86-2.38+7.14	$E_{OFFENSE}$ = -0.6+0+0.6+0
$E_{DEFENSE}$ = 28.57	$E_{OFFENSE}$ = 0

Company X. On the other hand, Team Offense receives no benefits or rewards for their participation in this game and leaves with nothing[3].

Using our matrix, we can illustrate the best strategies for each player based on the other side's strategies now that we know the payoffs for each player in all four possible outcomes. The matrix below shows the optimal responses from Team Defense highlighted in yellow, and the best replies from Team Offense highlighted in green (Table 3).

In our game scenario, the best strategy for Team Defense is to not defend the asset when Team Offense decides to attack it, and to defend it when Team Offense decides to not attack it. Team Offense's best strategies are to attack when Team Defense does not defend the resource, and to not attack when Team Defense decides to defend it. In this hypothetical game, the payouts for Team Def in the (Defend, Don't Attack) game are 25-1. There is no stable solution among the four possibilities, where both players are content with their current strategies and have no need to switch tactics offense, while the team score was. As a result, neither player has a dominant strategy that can increase their payoffs independently of the other player's strategy. Therefore, in this game, each player must choose their tactics randomly to maximize their expected rewards. To determine the optimal frequency of selecting each tactic, game theory principles can be applied, instead of using a coin toss to make strategy decisions[4].

We can use the variables p and q to represent the probability that Team Defense will defend the resource and Team Offense will attack it, respectively. By solving for these variables independently, we can determine the optimal strategies for each player that maximize their individual payoffs, regardless of how the other player chooses to play the game (Table 4).

Based on the calculations of p and q, we have concluded that both players can increase their payoffs if they decide to choose their tactics randomly. In this case, the optimal strategy for Team Defense would be to protect the asset 5 times out of 6, and for Team Offense, it would be to attack the asset once out of 7 times[5].

To estimate the expected rewards for each player in this game, we can calculate the anticipated payoffs for each player based on the probabilities of the four possible outcomes. To do this, we multiply the optimal strategies of each player by each other to determine the likelihood of each outcome occurring (Table 5).

So now we understand how frequently each one of the game's four possibilities will occur, we can determine the expected rewards for each participant, assuming they decide to participate in the game (Table 6).

The results of this hypothetical game are significant as they indicate that if Team Offense chooses to participate, they can expect to lose money. This implies that in reality, Team Offense is likely to avoid targeting Company X and look for other targets instead[6].

The rewards for participating in cyberwarfare games are likely to be dynamic due to the rapidly evolving nature of the cyber world. The value of information assets will change with the introduction of new technologies and outdated systems. Additionally, changes in the economy, political climate, consumer trends, and regulations can all affect the perceived value of participating in such games. To maintain an edge, Team Defense must continually evolve their approach if you want to know how vulnerable your company's data resources are, you need an exact list of all of your information assets, ranked by value to the business. Cybersecurity experts should implement measures to reduce the risk to their information assets to an acceptable level while optimizing their investment return using game theory concepts.

CONCLUSION

Game theory is a powerful tool in computer science for addressing security challenges. The previous sections demonstrate how game theory can be utilized to determine the optimal plays and strategies of players in order to achieve the best possible outcome for each individual. Cybersecurity uses game theoretic models to safeguard cyberspace against both physical and intrusion threats.

REFERENCES

1. Khouzani, M.H.R., P. Mardziel, C. Cid and M. Srivatsa, 2015. Picking vs. guessing secrets: A game-theoretic analysis. IEEE 28th Computer Security Foundations Symposium, January 01-01, 1970, IEEE, pp: 243-257.
2. Tosh, D.K., S. Sengupta, S. Mukhopadhyay, C.A. Kamhoua and K.A. Kwiat, 2015. Game theoretic modeling to enforce security information sharing among firms. IEEE 2nd International Conference on Cyber Security and Cloud Computing, November 03-05, 2015, IEEE, USA, pp: 7-12.
3. Pettet, G., S. Nannapaneni, B. Stadnick, A. Dubey and G. Biswas, 2017. Incident analysis and prediction using clustering and Bayesian network. IEEE SmartWorld, Ubiquitous Intelligence and Computing, Advanced and Trusted Computed, Scalable Computing and Communications, Cloud and Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI), August 04-08, 2017, IEEE, USA, pp: 1-8.
4. Magazinnik, A., 2007. Dynamic games of incomplete information., https://ocw.mit.edu/courses/17-810-game-theory-spring-2021/mit17_810s21_lec7.pdf
5. Vakilinia, I., D.K. Tosh and S. Sengupta, 2017. Privacy-preserving cybersecurity information exchange mechanism. International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS), July 09-12, 2017, IEEE, USA, pp: 1-7.
6. Rontidis, G., E. Panaousis, A. Laszka, T. Dagiuklas, P. Malacaria and T. Alpcan, 2015. A Game-Theoretic Approach for Minimizing Security Risks in the Internet-of-Things. IEEE International Conference on Communication Workshop (ICCW), June 08-12, 2015, IEEE, London, pp: 2639-2644.