Asian Journal of Research in Computer Science

Volume 16, Issue 3, Page 149-155, 2023; Article no.AJRCOS.95591
ISSN: 2581-8260

Gamified Cyber-Crime Monitoring and Control Framework in a Computer Network Environment

Sylvester Olatunji [a*], Boniface Alese [a], Olaniyi Ayeni [a] and Fabiyi Olakunle Olayinka [b]

[a] Federal University of Technology, Akure, Nigeria.
[b] Cardiff Metropolitan University, Cardiff, UK.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: 10.9734/AJRCOS/2023/v16i3352

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/95591

Short Research Article

Received: 10/11/2022
Accepted: 16/01/2023
Published: 22/07/2023

ABSTRACT

Recent advancements in cybercrime are continually emerging, with the estimated damages to the global economy reaching the billion dollar mark. In the past, people acting alone or in small groups were the main perpetrators of cybercrime. Complex cybercriminal networks are now bringing people from all over the world together in real time to commit crimes on a never-before-seen scale. Game theory gives a formal vocabulary for the description and study of interacting situations in which a number of "entities," known as players, take actions that have an effect on one another. The field of cyber security could benefit from problem-solving techniques based on games theory to protect assets. In this article, we suggest a conceptual framework for a system for monitoring and controlling cybercrime.

Keywords: Game theory; cybersecurity; cyber-crime; attacker; defender; cyber-warfare.

**Corresponding author: E-mail: olatunjisylvester@gmail.com, solatunji@futa.edu.ng;*

1. INTRODUCTION

It is crucial to understand cyber threats, manage risks, and develop effective preventive, defense, detection, analysis, investigation, and recovery strategies. Singer and Friedman in [1] highlighted the profitability of exploiting political, economic, and other terms, the simplicity and low cost of using resources to stage attacks, and the ease with which attackers can hide make it possible to carry out these activities anonymously and from anywhere in the world, are just a few of the factors that have been highlighted as contributing to the proliferation of criminal actions in cyberspace.

The term "cybercrime" refers to a wide range of illegal computer-related behavior. As the use of information technology increases, it gets more difficult to identify crimes that don't include the use of the internet. All types of criminal action that was partially or entirely enabled by cyberspace is referred to as cybercrime [2].

A rapidly expanding subset of crime is cybercrime. Numerous cybercriminals are taking advantage of the ease, speed, and anonymity of the Internet to engage in a wide variety of illegal activities that have no physical or virtual boundaries, do substantial harm, and present very real threats to victims throughout the internet. Cybercrime used to be primarily committed by individuals or small groups. Today, we see extremely sophisticated cybercriminal networks bringing together people from all over the world to perpetrate crimes on a never-before-seen scale. Criminal organizations are using the Internet more and more to facilitate their operations and increase their profit in the least amount of time. The crimes, which include theft, fraud, illicit gambling, and the sale of bogus pharmaceuticals, are not inherently new, but they are developing in response to the opportunities offered by the internet, making them more pervasive and destructive. Many cyber security risk assessment techniques place more of an emphasis on how vulnerable a system is to known exploits than on how to best defend against zero-day attacks [3].

A growing number of serious games have been created as a result of gamification approaches used in the security field. Anti-spyware and anti-virus software are no longer sufficient technologies to safeguard Internet users' accounts and PCs with the current volume of criminal activity on the Internet superhighway. Consequently, more levels of defense are required [4,5].

We have seen the introduction of new forms of security and privacy issues that directly impact network agents as networks take on a larger role in contemporary society. The significance of Network Security Stallings has considerably increased due to the enormous growth of the Internet. The risks to information and networks have increased significantly as networking and the Internet have developed. Game theoretic methods for assessing security have attracted a lot of study interest. A rapidly expanding subset of crime is cybercrime. Criminals are increasingly using the Internet's convenience, speed, and anonymity to perpetrate a wide variety of crimes that have no physical or virtual borders, inflict substantial harm, and present very real threats to victims all over the world.

We have seen the introduction of new forms of security and privacy issues that directly impact network agents as networks take on a larger role in contemporary society. The significance of Network Security Stallings has considerably increased due to the enormous growth of the Internet. The risks to information and networks have increased significantly as networking and the Internet have developed. Game theoretic methods for assessing security have attracted a lot of study interest. A rapidly expanding subset of crime is cybercrime. Criminals are increasingly using the Internet's convenience, speed, and anonymity to perpetrate a wide variety of crimes that have no physical or virtual borders, inflict substantial harm, and present very real threats to victims all over the world.

The paper contributions include:

We place a strong emphasis on the sometimes overlooked study of the dynamic interactions and evolution among cyber attackers and defenders.

Based on the generalized three-level attack/defense tactics game, we provide a non-cooperative zero-sum game to depict the cyberwarfare between attackers and defenders.

2. RELATED WORKS

Without taking into account (i) the dynamic attack intensity or the dynamic environmental conditions of the system, or (ii) the ongoing interactions between the attackers and the defenders where each of them is constantly adjusting its attack/defense strategies in order to gain the upper hand, most academic research has typically focused on a static model with a particular attack or defense on security. However, these two phenomena are present in practically all real-world cybersecurity issues.

Cybercrime is constantly changing, and the projected damages to the world economy are in the billions of dollars. Cybercrime used to be primarily committed by individuals or small groups. Today, we see extremely sophisticated cybercriminal networks bringing together people from all over the world to perpetrate crimes on a never-before-seen scale.

The study of mathematical representations of disagreement and collaboration between sane, rational decision-makers is known as game theory. In addition to logic in computer science and biology, game theory is mostly employed in economics, political science, and psychology. It first focused on zero-sum games, in which one player's gains cause losses for the other players. Game theory is currently a catch-all phrase for the study of logical decision-making in humans, animals, and computers that covers a wide range of behavioral relationships. The mathematical foundation for comprehending intelligent actors' interactions with one another has been provided by game-theoretic techniques, which makes the assumption that these intelligent actors will foresee one another's movements and behave appropriately [6].

There are two primary branches in game theory. The first is cooperative game theory, which makes the assumption that participants can interact with one another, establish alliances, and formally sign contracts. Political science and related subjects have used cooperative game theory, for instance, to examine voting patterns and other concerns. The non-cooperative game theory, however, simulates circumstances in which the players are either able to communicate but cannot sign binding contracts or are unable to communicate.

Game theory has been applied successfully in cyber security, particularly communication networks, to model a variety of difficulties [7,8]. Akinwumi et al in [9] presented a review of game theory approach in the management of cyber security risks. The process of managing or mitigating potentially harmful and unknown occurrences that pose dangers to cyber security is known as cyber security risk management. It entails examining potential cyberspace problems and choosing solutions to stop or lessen their occurrences or effects. Game Theoretic Approach (GTA) is a technique that is gaining increasing attention in managing cyber security risk, which focuses on the use of resources, internal controls, information sharing, technical improvements, behavioral or organizational scale-ups and cyber insurance for cyber risk management.

Musman and Turner in [10] outlined the models and approaches that make up the cyber security game. The study identified a method—cyber security game—as well as software that carries out the method. Which defense strategies and locations to be deployed are prescriptively defined in the study.

Hirschprung and Alkoby in [11] assessed the interactive nature of the information-sharing trade-off dilemma, a novel theoretical framework called Online Information-Sharing Assistance (OISA) was created. In the past few years, there has been an increase in interest in combining game theory with user behavior on social networks. Hu et al. in [12] applied a multiparty access control-based game theory model was used to elicit privacy issues in the context of online social networks. They did not, however, discuss the iterative choices that must be taken inside each activity.

Beckers and Pape in [13] proposed a game model that elicit security requirements and capture the underlying human behaviors targeted by social engineering. The players, who are divided into teams, learn attack and defense tactics based on human behavior and elicit security needs using the game cards as their guide. As the use of digital applications and the Internet continues to increase worldwide, Asswad & Marks in [14] introduced “associated risks to both privacy and security that threatens to violate individual data ownership”. Guo & Cho in [15] applied “a game theory framework to handle disinformation on social networks. The study reported how to effectively share information while considering the trade-off between the benefits and the resultant costs in information sharing environment”. Nilashi et al. in [16] proposed “recommender agents that support complicated decisions such as agents that assist travelers’ calls during the COVID-19 pandemic”. “Technological literacies are needed to understanding the complicated relationships between the actions taken in a digital space and their real-world consequences” [17]. “There is a significant gap between the actual privacy and security consequences of using technological applications and the users’ knowledge, expectations, and control of these consequences” [18].

Lacks of technological literacy makes it difficult for Individuals in online information-sharing environments to manage and control their own privacy and security. The stochastic nature of the problem and cognitive laziness make it more difficult to perceive [19].

In a non-cooperative attack-defense game, an attacker competes for the optimal action as a rational actor in the game, and his goal is to maximize his own utility. As a result, the adversaries are not required to collaborate with one another, which allows the malicious attacker to play the best possible game while wasting the system's resources. In contrast, the defender would also wish to employ an effective tactic to increase his chances of defending himself from the opposition without expending excessive energy or computational power on defending.

In this article, we model each participant with three levels of strategies: no attack/defense, low level of intensity, and high level of intensity, in order to provide a more comprehensive modeling of attackers/defenders where they can alter their attack/defense tactics with varied intensities.

Instead of having only two levels of tactics, as stated by the majority of the prior research, each attacker and defense have different levels of strategies in the proposed game framework. Each of the players in our model chooses either a low, moderate, or high level of intensity.

3. THE PROPOSED GAME MODEL

A two-player non-coordination zero-sum security game was considered which is represented by G =< (N),(S),(U) >, where N = {A, D} represents the two players: Player A is a malicious-node/attacker and the other player D is a defender. S = {ar, dr|r $\in$ {0, 1, 2}} is considered as the strategy space, which represent the set of actions that are available for each player, and their utilities are given by U.

During the game, both the attacker and the defender may employ one of the three tiers of strategy. level 0 for the attacker denotes his decision not to attack, denoted by a_0 =No-Attack, the first level is low intensity of attack, which is represented by a_1 = Attack-1; and the second level is a high intensity of attack, which is represented by a_2 = Attack-2. Basically, from the attacker’s perspective, compared with the strategy Attack-1, the strategy Attack-2 is more capable of producing successful attacks, but it requires more effort or resources from the attacker to put it into practice. Level zero for the defender, correspondingly, denotes his decision to take no defensive action, denoted by d_0 =No-Defend; level one is a low intensity of defense, denoted by d_1 =Defend-1; and level two is a high intensity of defense, denoted by d_2 =Defend-2. Therefore, the attacker A has three strategies: a_0=No-Attack, a_1=Attack-1, and a_2=Attack-2. The defender D has three strategies as well: d_0=No-Defend, d_1=Defend-1, and d_2=Defend-2. Assuming they are familiar with the game, both players decide on their plans simultaneously without consulting one another (i.e., U)/(gain and lost).

Assuming the value of the protected assets by the defender D to worth ω_n, where $\omega_n > 0$ and n $\in$ {1, 2}. ω_1 is the value of assets compromised by Attack-1 strategy deployed by the attacker successfully; ω_2 is the value of assets compromised by Attack-2 strategy deployed by the attacker successfully. According to zero-sum game, we assume that the gain of one player is equal to the loss of the opponent. Therefore, ω_n is the gain by the attacker if his strategy Attack-n is successful and $-\omega_n$ denotes the loss/damage by the defender. The amount of damage caused, such as energy wasted, the number of compromised or disabled nodes, the loss of data integrity, etc., is referred to as the value of this loss by the defender. The attacker and defender must both exert some work and expend some money in order to carry out their respective offensive and defense schemes. For the attacker, we denote the cost of attack as can where n $\in$ {1, 2}: c_{a1} is the cost to deploy Attack-1 strategy, and c_{a2} is the cost to deploy Attack-2 strategy. Likewise, for the defender, we denote the cost of defense as c_{dn} where n $\in$ {1, 2}: c_{d1} is the cost to deploy Defend-1 strategy, and c_{d2} is the cost to deploy Defend-2 strategy.

Table 1 illustrates the payoff matrix of the game in a strategic form.

Fig. 1 depicts the extensive form of the attack-defense game in the proposed framework.

Table 1. Strategic form of attack-defense game

	d_o	d_1	d_2
a_o	0,0	c_{d1}, - c_{d2}	c_{d2}, - c_{d2}
a_1	$w_1 - c_{a1}$, $c_{a1} - w_1$	c_{d1} - c_{a1} , c_{a1} - c_{d1}	c_{d2} - c_{a1} , c_{a1} - c_{d2}
a_2	$w_2 - c_{a2}$, c_{a2} - w_2	$w_2 + c_{d1} - c_{a2}$, c_{a2} - c_{d1} - w_2	c_{d2} - c_{a2} , c_{a2} - c_{d2}

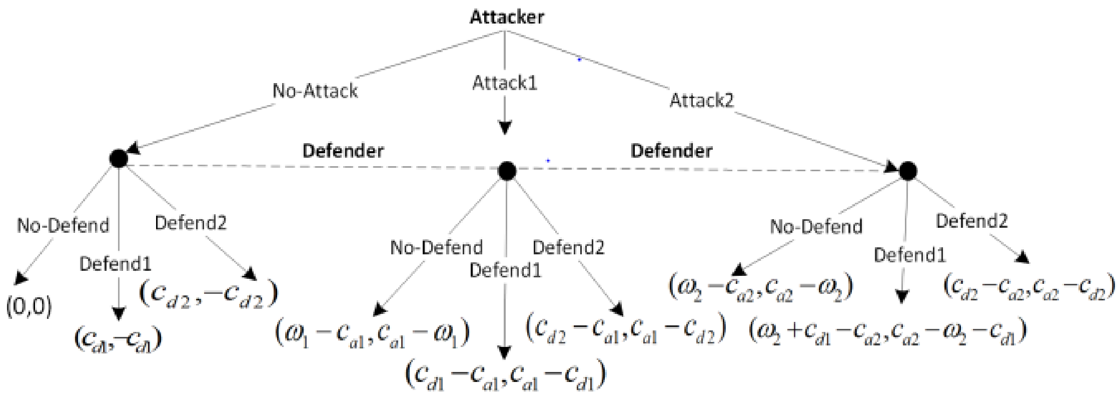

Fig. 1. Attack-defense cyber security game

4. MODEL ASSUMPTIONS

For our suggested three-level attack/defense strategy model, we assume the following:

i. The value of security assets is always larger than the cost to protect or attack against them since, in the absence of this, neither the defender nor the attacker would be motivated to do so, respectively; i.e, $\omega_n > c_{an}, c_{dn}$, $n \in \{1, 2\}$.
ii. Cost of attack strategy a_1=Attack-1 is less than the cost of attack strategy a_2 =Attack-2 for the attacker. Since Attack-2 is a more aggressive and effective attack strategy than Attack-1, Attack-2 takes more attacking efforts or cost to deploy. (i.e., $c_{a1} < c_{a2}$).
iii. Cost of defense strategy d_1 =Defend-1 is less than the cost of strategy d_2 =Defend-2 for the defender. Again, this is because Defend-2 is a more aggressive and effective defense strategy than Defend-1. (i.e., $c_{d1} < c_{d2}$).

A more aggressive/effective attack will typically result in greater damage being done to a target if it is successful. Thus based on the definition of ω_n in previous subsection, it is safe to assume that ($\omega_2 \geq \omega_1$).

The Mixed Strategy Nash Equilibrium of the security game is a probability distribution Ṕ over the set of pure strategies S for any player such that:

$$\acute{P} = (p_1, p_2, p_3, \dots, p_r) \epsilon R^{\bar{R}} \geq 0, and \sum_{t=1}^{\bar{R}} p_t = 1 \quad (1)$$

For the attacker, let p_{a0} be the probability of playing strategy a_0, p_{a1} be the probability of playing strategy a_1, and $p_{a2} = 1 - p_{a0} - p_{a1}$ be the probability for playing strategy a_2 for the attacker. In the same manner, for the defender let p_{d0} be the probability of playing strategy d_0, p_{d1} be the probability of playing strategy d_1, and p_{d2}=1−p_{d1}−p_{d2} be the probability for playing strategy d_2.

According to the Mixed Strategy Nash Equilibrium definition, the opponents become indifferent about the choice of their strategies by making the expected payoffs equal. Consequently, in our suggested game, the mixed strategy renders each player uninterested in any of their three methods when the expected utilities from playing strategies a_0, a_1, and a_2 are equal for the attacker, and the expected utilities from playing strategies d_0, d_1, and d_2 are equal for the defender, i.e.,

$$EU(p_{a_o}) = EU(P_{a_1}) = EU(p_{a_2}) \quad (2)$$

$$\mathrm{EU}(p_{d_o}) = \mathrm{EU}(P_{d_1}) = \mathrm{EU}(p_{d_2}) \quad (3)$$

Table 2. Strategic form of the attack-defense game with two strategies defender (D)

		d_o	d_1
Attacker (A)	a_o	0, 0	c_{d2} , - c_{d2}
	a_2	$w_2 - c_{a2}$, c_{a2} - w_2	$c_{d2} - c_{a2}$, c_{a2} - c_{d2}

Table 2 illustrates the payoff matrix of the game with two strategies form.

The distribution $\{p_{a0}$, $p_{a2} = 1 - p_{a0}\}$ for the attacker, and $\{p_{d0}$, $p_{d2} = 1 - p_{d0}\}$ for the defender are mixed strategy NE for the non-cooperative security game. In this scenario, each player will choose two strategies at random in accordance with the probability distribution and will not care how the play turns out.

We calculate the predicted utility as a function of the mixed approach which is expressed as:

$$\mathrm{EU}(p_{d_o}) = (P_{a_o})(0) += p_{a_2}(c_{a2} - w_2) \quad (4)$$

$$\mathrm{EU}(p_{d_2}) = (P_{a_o})(-c_{d2}) + p_{a_2}(c_{a2} - w_2)$$

The expected utility of the defender for playing strategy d0, and d2 are a function of the mixed strategy which are given by:

$$\mathrm{EU}(p_{a_o}) = (P_{d_o})(0) += p_{a_2}(c_{d2}) \quad (5)$$

$$\mathrm{EU}(p_{a_2}) = (P_{a_o})(w_2 - c_{a2}) + p_{d_2}(c_{d2} - c_{a2})$$

The expected utilities of playing the two strategies of each player are equal and no player has incentive to change his strategy. Therefore,

$$\mathrm{EU}(p_{d_o}) = \mathrm{EU}(p_{d_2}) \quad (6)$$

$$\mathrm{EU}(p_{a_0}) = \mathrm{EU}(p_{a_2}) \quad (7)$$

5. DISCUSSION

Without any informative framework, cyber war gamers frequently struggle to choose a logical, comprehensible approach that will reduce chances of attacks during interaction on the computer network. Varied levels of intensities was considered in the model to provide three levels of tactics to the players. In the model, players can only choose one option out of the three tactics. Some assumptions were made in the model in order to accommodate the dynamics of the security game. The Mixed Strategy Nash Equilibrium and pay off matrix were discussed accordingly. The values of the computation would be obtained during implementation which is the next phase of the study.

6. CONCLUSION

In order to simulate the ongoing and changing interactions and cyberwar activities between attackers and defenders, we proposed in this study a gamified framework for attack-defense security games in a computer network environment. To give a generalized modeling of the strategic decisions made by attackers and defenders, a three-level attack/defense strategy was employed to describe the game. From the game model, a mixed Nash equilibrium strategy was developed. This study takes a novel approach to network security and cybersecurity by combining game theory, inequality theory, and expected utility of decision-makers. The players can make an informed decision on the best course of action by using this analytical method to engage in a logical review of their options. The study is limited to the designed framework for cyber-crime monitoring and control. In the future study, implementation of the proposed framework on both hypothetical and real life networks would be carried out.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Singer PW, Friedman A. Cybersecurity and cyberwar: What everybody needs to know. NY: Oxford Univeristy Press; 2014.
2. Grobler M, Vuuren JJ, Zaaiman J. Cyber crime and cyber warfare with international cyber collaboration for RSA – Preparing communities. Council for Scientific and Industrial Research; 2013.
3. Jajodia S, Noel S. Topological vulnerability analysis. In: Cyber situational awareness. Boston, MA: Springer. 2010;139–154.
4. Cruz A. Cyber crime and how it affects you. Monthly Newsletter. 2013;7(1).
5. Halder D, Jaishankar K. Cyber crime and the victimization of women: Laws, rights and regulations. Information Science Reference; 2012.

6. Milind T, Manish J. Introduction and overview of security games. University of Southern California: Cambridge University Press; 2011.
7. Wang Y, Wang Y, Liu J, Huang Z, Xie P. A survey of game theoretic methods for cyber security, in IEEE First International Conference on Data Science in Cyberspace (DSC); 2016.
8. Chukwudi AE, Udoka ICE. Game theory basics and its application in cyber security, Advances in Wireless Communications and Networks. 2017;3(4):45–49.
9. Akinwumi DA, Iwasokun GB, Alese BK, Oluwadare SA. A review of game theory approach to cyber security risk management. Nigerian Journal of Technology (NIJOTECH); 2017.
10. Musman S, Turner A. A game theoretic approach to cyber security risk management, Journal of Defense Modeling and Simulation: Applications, Methodology, Technology; 2018.
11. Hirschprung RS and Alkoby S. A game theory approach for assisting humans in online information-sharing, MDPI; 2022.
12. Hu H, Ahn G, Zhao Z and Yang D. Game theoretic analysis of multiparty access control in online social networks. In Proceedings of the 19th ACM Symposium on Access Control Models and Technologies, New York, NY, USA. 2014;93–102.
13. Beckers K, Pape S. A serious game for eliciting social engineering security requirements, in: 24th International Conference in Requirements Engineering, IEEE. 2016;16–25.
14. Asswad J, Marks JG. Data ownership: A survey. Information. 2021;12:465.
15. Guo Z, Cho J. Game theoretic opinion models and their application in processing disinformation. In Proceedings of the 2021 IEEE Global Communications Conference (GLOBECOM), Madrid, Spain. 2021;7–11:1–7.
16. Nilashi M, Asadi S, Minaei-Bidgoli B, Abumalloh RA, Samad S, Ghabban F, Ahani A. Recommendation agents and information sharing through social media for coronavirus outbreak. Telemat. Inform; 2021.
17. Desimpelaere L, Hudders L, Sompel D. Knowledge as a strategy for privacy protection: How a privacy literacy training affects children's online disclosure behaviour. Comput. Hum. Behav; 2020.
18. Brough AR, Martin KD. Critical roles of knowledge and motivation in privacy research. Curr. Opin. Psychol. 2020;31: 11–15.
19. Puaschunder JA. Utility theory of privacy and information sharing. In Encyclopedia of Information Science and Technology, 5th ed.; IGI Global: Hershey, PA, USA. 2021;428–448.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/95591