A Theoretical Game Approach to Attacker-Defender Interaction

[1]Yetunde Ogunlola, [2]Otasowie Owolafe, [3]Aderonke F. Thompson, [3]Adewale Oronti, [5]Boniface K. Alese
[1]Computer Science Department, [2, 3, 4, 5]Cyber Security Department
Federal University of Technology, Akure

Abstract

This research presents modeling cyber-attack as a game simulated approach that shows the interaction between attacker and defender in cyberspace. Game theory provides a foundational approach for network security investigation and simulation. The research was motivated by the issues presented by the various techniques that have been developed for modeling the interactions between internet users and cyber attackers in cyberspace. One of the most effective techniques researchers have been exploring is the application of game-theoretic approaches to address network and security issues in the cyber world. Previous research did not consider the evolving nature of the attacker and defender interaction. This research, therefore, focused on the development of a 2D mobile and desktop game simulation model for cyber-security using the game theory model by elaborating the attacker and defender activities in a networking environment. The security game model aimed at constructing a typical network environment and its risk assessment framework where the intention of each player is to maximize his or her payoff or minimize his or her loss as much as possible. The result of the simulation shows that interactive games can be a promising way of modeling the interaction between attacker and defender and proffering ways to avoid falling for cyber-attacks.

1. Introduction

Technological advancements in computing environments and computer applications have led to the development of networks and unregulated social networking which give rise to thousands of active users and applications at any given time. Many of these users and applications are not secured, hence, there exist cybercriminals, masquerades, hackers and antisocial persons seeking to exploit system vulnerabilities, particularly in the educational environments [1]. Man has grown to depend on the Internet on a continual basis and have incorporated it into their lives. As a result of this dependence, hackers have also made the Internet a potential attack platform [2]. The dynamic nature of both the attackers and defender in an intelligent environment has bought a lot of dynamism in attack, hence, corresponding dynamism in defense leading to the concept of Cyber war Gaming. Cyber War Gaming is an interactive exercise that immerses participants in a simulated cyber-attack scenario, such as a data breach, website defacement, denial of service attack, or the discovery of sophisticated malware on a corporate network. Cyber War Gaming is a cyber security incident around the world, and has necessitated the need for research in Information and Cyber security [3]. Apparently, checking through the advancement of network security, cyber attackers cannot be stopped by purely static measures such as classical firewalls. When targeting the vulnerabilities of networks, attackers update their strategies daily. Hence, it is crucial for the defense to also take dynamic measures and address security both in the design phase and afterwards.

Games used for teaching are referred to as game-based learning methods and they serve as a tool for complementing the traditional teaching methods to improve learning experience of students [4]. The game-based learning method helps students improve problem-solving skills and make it possible for them to interpret their society, nature and the world around them through experiences [5]. Learning through mobile games is an educational process where the users are required to perform learning activities by using a game or a series of games designed for specific learning activity. In a study focused on gaming for learning, it was identified that learning process can be significantly improved by mobile gaming education [6]. Research has also found that games are effective educational tools widely popular and effective in teaching, especially, puzzle games.
Dynamic game is a game in which players move sequentially or repeatedly. It is a game with complete information unlike a static game where information is incomplete. A dynamic game is a game with more than one stage in each of which the players can consider their action [7]. Most academic research have typically focused on a static model with a particular attack or defense on security without considering [8] the following phenomena:

(i) the dynamic attack intensity or the dynamic environmental conditions of the system;

(ii) the continuous 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.

However, these two phenomena exist in almost all cybersecurity problems in the real world. Thus, besides having a specific defense algorithm, it is equally or even more important to design a defense system that can adjust its strategies to achieve the best defense performance against intelligent attackers and defenders under various attack situations.

2. Related Works

The internet has turned into a safe abode for smart criminals who are persuaded by significant monetary or political gain [9]. Poor modeling of the activities of these intelligent criminals in the cyber space allows them to effectively target users of computing devices. Modeling the activities of these criminal minded individuals will provide defenders measures to put in place in other to avoid these attacks. Researchers such as [10], [7], [11] and others have worked on the use of game theory and game-based approaches for cybersecurity. These studies with their drawbacks are documented as follows:

In 2020, Mahmoud et al. [7] performed a study on combining game-based learning with virtual cyber labs. The authors presented architecture of a new platform, designed for user-friendly and automated generation of complex gaming scenarios for learning about cybersecurity. This enabled the creation of realistic scenarios for training both technical skills and the participants' abilities to act and make decisions in stressful situations. Additionally, the study offered the possibility for users to interact with each other, both within and between teams, raising their abilities to communicate and solve challenges. The drawback of the study was that, the design failed to incorporate design elements from well-known information system theories.

The author in [12] presented an experimental gaming model based on learning theory, flow theory and game design. The researchers used the flow theory to enable positive user experience for the maximization of the impact of educational games. The designed model provided players with immediate feedback, clear goals and challenges matched to player's skills. The model was seen to create a positively competitive environment. The design flow of the game was not easily understandable, hence, players found it difficult to understand the gaming concepts.

[10] performed a game-based learning evaluation using a quasi-experimental design with 458 pupils from 20 classes from five schools. The pupils in 10 of the classes played the mobile history game whereas the pupils in the other 10 classes received a regular, project-based lesson series. Results showed those pupils who were engaged in the game gained significantly more knowledge about the history of Amsterdam than pupils who received regular project-based lessons. A major drawback was the failure of the research to allow individual story construction and the addition of elements of the pupils' interests. Hence, the interest of the pupils in the game eventually decreased since the story line and assignments could minimally be influenced by players.

The authors in [11] designed an augmented reality game for cybersecurity awareness that teaches not only cybersecurity concepts but also demonstrates the consequences of actual cybersecurity attacks through feedback. The real-time discussion and analysis of learning topics through interactive games was seen to strengthen the player's attentiveness to cybersecurity awareness. To evaluate the effectiveness of the game, a survey was conducted. The responses from the survey indicated that the game was useful for players to develop an understanding of cybersecurity attacks and vulnerabilities. However, the game was not aligned with the curriculum of the students.

In 2018, [13] used behavioral game theory for investigating the role of certain actions taken by attackers and defenders in a simulated cyber-attack scenario of defacing a website. The researchers used Reinforcement Learning (RL) model to represent a simulated attacker and a defender in a 2x4 cyber-security game, where players could take up to 4 actions. In order to evaluate the performance of the model, participants were computationally simulated across 1000 simulations, where players played at most 30 rounds in the game. The attacker was tasked with defacing the website while the defender was to prevent the attacker from doing so. Results showed that the model performed well yet, setting up was costly and required higher logistics.

A multiplayer computer game for teaching cybersecurity concepts to students was presented by [10]. The game called Security Empire, challenges users to build a green energy company while engaging in cybersecurity practices and avoiding unsafe practices such as clicking on unsafe links, decrypting auction bids, not authenticating software downloads, not performing integrity checks of system software, keeping antivirus protection outdated, and using weak passwords. A pilot of the game was used in a high school and results showed that it was engaging and increased cybersecurity awareness. However, a major drawback was that, dynamics in the game were difficult to align with learning objectives as to meet the educational model.

In a study by [15], a cybersecurity game-based learning design using the elaborated action design research approach (e-ADR) was presented. The game teaches players about incident detection and handling procedures needed to be undertaken in the event of a cyber-threat. Although the game was aimed at training players in cybersecurity forensics by focusing on detection and containment phases, the other phases of the National Institute for Standards

and Technology (NIST) incidence response life cycle such as preparation and post-event activity phases were not considered.

The author in [16] used CyberCIEGE to investigate the application of cyber security concepts amongst graduate students. The researchers used 20 scenarios with each of them describing the concept of network security. For this analysis, a study was conducted on 20 engineering graduate students offering a formal cyber security curriculum divided into 2 control groups. The first control group which contained 10 graduate students were tested without playing the game and the other control group which also comprises of 10 graduate students were tested after playing the game. The results displayed a better learning outcome for the group that played the game before the taking the test.

The researchers in [17] introduced a gaming approach to India Capture the Flag (InCTF) with an objective to learn cybersecurity at various levels, testing the knowledge of students on the concept of cybersecurity at the various times. The authors introduced three rounds of learning: the learning round which majored on the introduction of the concepts of cybersecurity; the jeopardy round which involved testing the knowledge of participants based on the learning round through a gaming approach which divided the game into various levels; and the interactive round which also involved the application of cyber security in the real-world scenario through the creation of virtual images. The game provided each team with an understanding of their vulnerabilities so as to be able to attack other teams and defend their own systems from incoming attacks.

3. System Design

The security game system's model aimed at constructing a typical network environment and its risk assessment framework. Since the game model is centered on an attacker and a defender interaction in a computer network environment and the intention of each player is to maximize his or her payoff or minimize his or her loss as much as possible. The system uses Mixed Strategy Nash Equilibrium for two-level strategies technique to model the interaction between the attackers and the defenders.

3.1. Game Model

The design of the game is adopted as an operational mode of the networked system, in which units are fully, partially operational, or completely out of operation. Each player selects actions from available action space with the goal of maximizing the payoff. The state of a network is modeled as one containing various kinds of information or features such as type of hardware, software, connectivity, bandwidth and user privileges. The game transit from one state to another according to a probability distribution and being an attack-defense game model, which quantifies the probability of threats, is formulated for the risk assessment. Since the proposed game model is centered on an attacker and a defender interaction in a computer network environment, a two-player zero-sum security game will be considered, represented by

$$G = \{(N), (S), (U)\} \quad (1)$$

Where **N** represents the two players: Player A is a malicious-node/attacker and the other player is a defender.

$$N = \{A, D\} \quad (2)$$

S is the strategy space, which is the set of actions that are available for each player, and their utilities are given by U.

$$S = \{ar, dr | r \in \{0, 1, 2\}\} \quad (3)$$

the intention of each player is to maximize his or her wins or minimize his or her loss as much as possible, a strategic tuple G is therefore defined as:

$$G = (n, Ai, Ri) \quad (4)$$

Where "n" is the number of players, i = 1, 2, …, j
"Ai" is the set of actions or strategy space available to a player and "Ri" is the player's payoff function A R.
These are often called matrix game because the Ri can be written as n-dimensional matrices. The following assumptions for the proposed two levels attack-defense strategy model is given in Table 1.

Table 1: Strategic form of Attack-Defense game.

	Defender D	
Attacker (A)	d_0 (No Defend)	d_1 (Defend)
a_0 (No attack)	0, 0	cd_1, $-cd_1$
a_1(Attack)	$\omega_1 - ca_1$, $ca_1 - \omega_1$	$cd_1 - ca_1$, $ca_1 - cd_1$

The game model requires a definition of what the outcome when the attacker deploys one specific attack strategy and the defender implements one specific defense strategy. The following assumptions are made on the game outcomes:

i. Attack is successful under these scenarios: Attack vs. No-Defend;

ii. Defense is successful under these scenarios: Defend vs. Attack or No-Attack.

iii. Zero gain or loss when there is no attack and no defense deployed, i.e., No-Attack vs. No-Defend.

The above assumptions mean that the more aggressive defense strategy, Defend, is secure against all attacks. However, No-defense strategy, is still vulnerable to be dealt with by the aggressive attack, Attack.

Table 2 illustrates the payoff matrix of the game in a strategic form being a deterministic, nonzero sum payoff matrix game with a win for one not necessarily implying a loss for the opponent. The matrix game played for the attacker and the defender is made up of rows and columns.

Table 2. Payoff Matrix

	Player 2			
Player 1	1	2	3	4
1	4	0	6	-2
2	2	6	1	1

For this security game, there is no Pure Strategy Nash Equilibrium where each player in the game always has the incentive to deviate to another strategy in order to gain higher payoff. Therefore, Mixed Strategy Nash Equilibrium will be used for the model.

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

$P = (p_1, p_2, p_3, ..., p_r) \in R^R \geq 0$, and $\sum_{t=1}^{R} pt = 1$ (5)

In this case, each player will randomize his selection of two strategies conformity with the probability distribution and he will be indifferent about the outcomes of the play as well. Therefore, the MSNE of this model is for two-level strategies. For the attacker, let p_{a0} be the probability of playing strategy a0, and $p_{a1} = 1 - p_{a0}$ be the probability for playing strategy a1 for the attacker. In the same manner, for the defender let p_{d0} be the probability of playing strategy d0, and $p_{d1}=1-p_{d0}$ be the probability for playing strategy d1.

According to the MSNE definition, the opponents become indifferent about the choice of their strategies by making the expected payoffs equal. Therefore, in this game, the mixed strategy makes player indifferent among all two of their strategies when the expected utilities from playing strategies a0, and a1 are equal for the attacker, and the expected utilities from playing strategies d0, and d1 are equal for the defender, that is,

$EU(p_{a0}) = EU(p_{a1})$ (6)

$EU(p_{d0}) = EU(p_{d1})$ (7)

Then, the expected utility of the attacker for playing strategy a0, and a1 as function of the mixed strategy is calculated and are given by:

$EU(p_{a0}) = (p_{d0})(0) + p_{d1}(c_{d1})$ (8)

$EU(p_{a1}) = (p_{d0})(\omega_1 - c_{a1}) + p_{d1}(c_{d1} - c_{a1})$ (9)

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

$EU(p_{d0}) = (p_{a0})(0) + p_{a1}(c_{a1} - \omega 1)$ (10)

$EU(p_{d1}) = (p_{a0})(-c_{d1}) + p_{a1}(c_{a1} - \omega 1)$ (11)

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

$EU(p_{a0}) = EU(p_{a1})$ (12)

$EU(p_{d0}) = EU(p_{d1})$ (13)

Then, substituting (8), and (9) in (10), and (11), and (12) in (13) and solving the expression in order to find the probabilities that correspond to the equilibrium, results:

$p_{a0} = \omega_1 - c_{d1}\,\omega_1$, $p_{a1} = 1 - \omega_1 - c_{d1}\,\omega_1$ (14)

$p_{d0} = c_{d1}\,\omega_1$, $p_{d1} = 1 - c_{d1}\,\omega_1$ (15)

4. System Implementation

The experiment demonstrates how game theory can be implemented in a 2D game for cyber security training and creating awareness in an interactive manner. The game plot is based on different types of cyberattacks. The attacks include malware attacks, password hacking, virus, and unauthorized data. The game depicts a scene where the player defend itself from attackers either by attacking or escaping through. The cyber attackers or hackers are attacking the player with malicious content. The success and payoff are measured in the terms of distance travelled by the player, the number of cyber attackers been attacked or how fast to response in defense.

Figure 1. Menu page

The Scene layout of the game as shown in Figure 2 illustrate how the game is been built on the unity engine and every item needed for the development of the game.

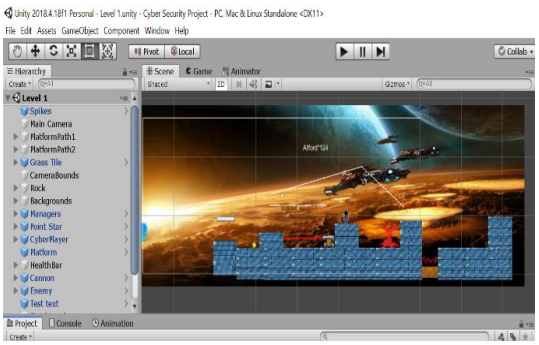

Figure 2. Scene Layer for the game building

Figure 3 illustrates the level 1 scene where the player encounters the virus and trojan attacks. In this scenario the player has two options. Either he/she can dodge the attack or can use their ally which is antivirus icon. This antivirus will make the player attack his/her attacker which increase the player payoff and access to move to the next level. Apparently, if the playeris active to defend itself from the virus and trojan, then its strength reduces and eventually pack up which means, game restart.

Figure 3. Game Layout for Level 1

The level 2 and level 3 scene represented in Figure 4 and Figure 5 represents the unauthorized data, which an attacker is trying to penetrate in player's computer. The player can either hit this enemy or can choose firewall icon to kill it enemies.

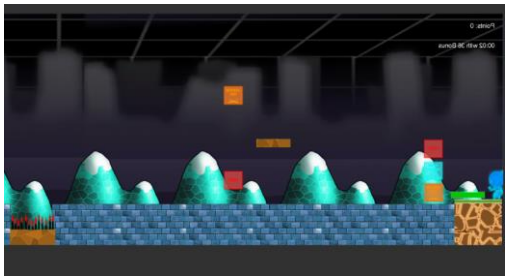

Figure 4. Level 2 Game layout

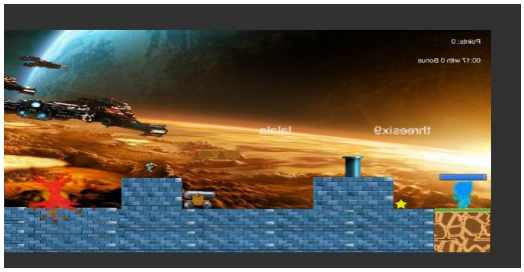

Figure 5. Level 3 Game Layout

Characters
The characters used in this project are in two forms;
The Main Characters: These are the players of the game as shown in Figure 6.

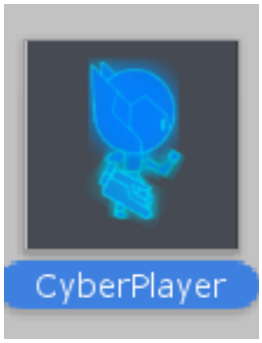

Figure 6. Player

The Enemy Characters: These are the cyber attackers. They do not chase the player but can shoot single or multiple projectiles and only move in either horizontal or vertical direction. There is in total 8 enemies in the game, each have different animations, health, damage to challenge the player. The enemy character can be seen in Figure 7.

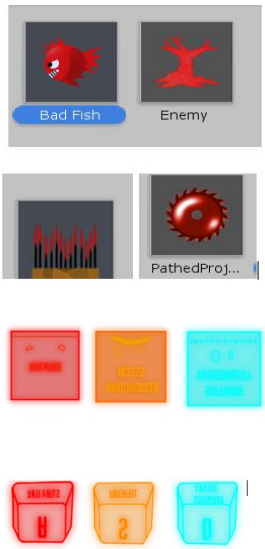

Figure 7. Enemies such as Virus, unauthorized access and Software Vulnerability

4.2. Result

The main aim of this designed model to is prove it as teaching methodology of cyber security in a network environment. The player playing this game recognizes the icons and gets familiar with them to play the game. The familiarity with icons such as the enemies (attackers), their moves, form of attacks and what countermeasures can be used to encounter them makes the player learn about the cybersecurity. The player understands and encounters the challenges in this game. The success of each level in this game is every move of defense by the player and attack to it enemies. Also, to every attack the player receives from its enemies, it loses more point.

4.3. Comparative Analysis of Model with Existing Work

The performance of the Cyber Security gaming System is evaluated with the Game theoretic model proposed in [15]. The evaluation of the models is presented in Table 3.

5. Conclusion

As the general population becomes increasingly refined in their understanding and use of computers and as the technologies associated with computing become more powerful, there is a strong possibility that cyber-crimes will keep increasing. Cyber security must be addressed seriously as it is affecting many internet users. The attackers can operate without detection for years and can remain hidden from any counter measures. Reason why an internet user (the defender) must be alert and ready to defend every data. Incorporating games into learning has proven to improve the learning outcome overtime.

6. References

[1] Manousos, E. (2020), "Stop thinking of cybersecurity as a problem: Think of it as a game", https://www.helpnetsecurity.com/2020/11/11/cybersecurity-game/, (Access Date: June 8, 2021).

[2] Hichem Sedjelmaci, Makhlouf Hadji, and Nirwan Ansari, (2019), "Cyber Security Game for Intelligent Transportation Systems", IEEE Network, vol. 33, no. 4, pp. 216-222.

[3] Center for Internet Security. The CIS security metrics. May 2009.

[4] Tolulope Awojana and Te-Shun Chou (Department of Technology Systems College of Engineering and Technology East Carolina University). "Overview of Learning Cybersecurity Through Game Based Systems".

[5] Sukran, U. (2015), "Elementary School Teachers' Views on Game-based Learning as a Teaching Method", Procedia - Social and Behavioral Sciences, Vol. 186, pp. 401 – 409.

[6] Nagarajan, A., Allbeck, J. M. and Sood, A. (2012), "Exploring Game Design for Cybersecurity Training", Proceedings of the 2012 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, pp. 256 – 262.

[7] Mahmoud, R., Kidmose, E., Broholm, R., Pilawka, O. P., Dominika, I. D., Magnussen, R. and Pedersen, J. M. (2020), "Attack and Defend: Combining Game-Based Learning with Virtual Cyber Labs", Proceedings of the 14th European Conference on Games Based Learning, 10 pp.

[8] Afraa Attiah, Mainak Chatterjee, Cliff C. Zou. (2013). (College of Engineering and Computer Science, University of Central Florida, Florida, USA). "A Game Theoretic Approach to Model Cyber Attack and Defense Strategies".

[9] Yu Shui, Wang Guojun, and Zhou Wanlei. (2015), Modeling Malicious Activities in Cyber Space. IEEE Network Vol. 29(6), pp 83-87, 2015.

[10] Huizenga, J., Admiraal, W., Akkerman, S. and Dam, G. (2009), "Mobile game-based learning in secondary education: engagement, motivation and learning in a mobile city game", Journal of Computer Assisted Learning, Vol. 25, pp. 332–344.

[11] Hamed, A. and Manolya, K. (2020), "Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR)",Journal of Information Science and Technology, Vol. 11, No. 2, 19 pp.

[12] Kiili, K. (2005), "Digital game-based learning: Towards an experiential gaming model", Journal of Internet and Higher Education, Vol. 8, pp. 13–24.

[13] Vinod K. Aggarwal & Andrew W. Reddie (2018) Comparative industrial policy and cybersecurity: a framework for analysis, Journal of Cyber Policy, 3:3, 452-466, DOI: 10.1080/23738871.2018.1553989.

[14] Olano, M., Sherman, A., Oliva, L., Cox, R., Firestone, D., Kubik, O., Patil, M., Seymour, J., Sohn, I., Thomas, D. (2014). {SecurityEmpire}: Development and Evaluation of a Digital Game to Promote Cybersecurity Education. In proceeding of the 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14), San Diego, CA.

[15] Dixon Prem and Daniel Rajendran (2020). An e-ADR (elaborated Action Design Research) Approach Towards Game-based Learning in Cybersecurity Incident Detection and Handling. In proceedings of the 53rd Hawaii International Conference on System Sciences, pp 5066-5075. DOI:10.24251/HICSS.2020.623.

[16] Raman, R., Lal, A. & Achuthan, K. (2014). Serious Games Based Approach to Cyber Security

Concept Learning: Indian Context. Semantic Scholar.

[17] Boopathi, K., Sreejith, S. & Bithin, A. (2015). Learning Cyber Security Through Gamification. Indian Journal of Science and Technology, Vol. 8(7), 642-649.

Table 3. Comparative Analysis

S/N	PERFORMANCE ANALYSIS	GAME THEORETIC APPROACH PROPOSED IN THE GAME	GAME THEORETIC APPROACH PROPOSED IN (Dixon and Sundarraj (2020).
1.	Scalability	Scalable to accommodate the complexity of changes in cyber-attack.	No Scalable
2.	Processes	Consider cyber-attacks as a continual process.	Consider incident detection and handling procedures to be undertaken in cyber events only.
3.	Attacks	Considered more cyber-attacks. For example, SQL injection, malware and RDDoS attacks	It only considered incident detection and procedural handling
4.	Payoff	During cyber-attacks, it is not only the bandwidth that is affected by the attack. The memory and processor are also affected. This has been incorporated in the players' payoff functions in this research.	No payoff