Web security assessment and strategy optimization based on attack-defense game

Wenfei Yu
Beijing University of Posts and Telecommunications
Zigang Chen (chenzg@cqupt.edu.cn)
Chongqing University of Posts and Telecommunications

Research Article

Keywords: Game theory, Web vulnerability, Different capabilities, OWASP, Nash equilibrium, Matrix

Posted Date: May 18th, 2022

DOI: https://doi.org/10.21203/rs.3.rs-1640559/v1

Web security assessment and strategy optimization based on attack-defense game

Wenfei Yu[1], Zigang Chen[2,*]

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876 China.

[2] Chongqing Key Laboratory of Cyberspace and Information Security, Chongqing University of Posts and Telecommunications, Chongqing 400065 China.

[*]Corresponding author: Zigang Chen. E-mail: chenzg@cqupt.edu.cn

Abstract

Based on game theory, we analyse the attack-defence process between penetration testers and system defenders related to web vulnerabilities, and we propose a web security assessment and strategy optimisation based on attack-defence games. First, according to the actual process of the network, we build a web attack-defence game model that considers the multiple influence parameters of web vulnerabilities on the profitability of attack and defence. These parameters include the difficulty of vulnerability exploitation and detection, the influence of vulnerability hazards, and the prevalence of vulnerabilities. In addition, we quantify the decision cost and the ability of both attack and defence subjects using the Nash equilibrium principle to obtain the best attack and defence strategies corresponding to the defender. Experiments verified the effectiveness of the model proposed in this paper, focusing on the specific impact of the different capabilities of the two parties and the different decision costs of the benefits. This can not only enhance the penetration success rate of the penetration tester but also allow the system defender to make targeted defence enhancements to the system based on the defence payoff matrix.

Keywords: Game theory; Web vulnerability; Different capabilities; OWASP; Nash equilibrium; Matrix

Conflict of Interests

The authors declare that they have no conflict of interest.

Acknowledgement

This work was supported in part by Open Foundation of State key Laboratory of Networking and

Switching Technology (Beijing University of Posts and Telecommunications) under Grant SKLNST-2020-1-15, and in part by introduction of talent research start-up fund of Chongqing University of Posts and Telecommunications under Grant E012A2020210.

Author's contributions

Conceptualization, Yu.W.F, Chen.Z.G.; methodology, Yu.W.F; writing—original draft preparation, Yu.W.F; contribution to contents, review and editing, Chen.Z.G.; supervision, Chen.Z.G. All authors have read and agreed to the published version of the manuscript.

1 Introduction

Information and network techniques are currently developing rapidly [1] because networks are inextricably interwoven with people's lives and productivity [2], and they play an influential role in various fields. Moreover, network security issues have become more conspicuous [3], and the scale of network attacks has become increasingly complex. Network security incidents may even affect world economic security [4]. Recently, Beijing Rising Network Security Technology Co. LTD announced the ' 2020 China Cyber Security Report ', in which more than 148 million samples of computer malware were captured in 2020.The number of computer virus infections was 352 million, and the total number of viruses was 43.71% higher than that in 2019 [5]. Network security problems are becoming increasingly severe, and the frequency and types of network security incidents are also increasing, especially in web vulnerabilities. The attack methods and paths are trending toward complexity, and the corresponding vulnerabilities are also becoming more diverse, which further aggravates the security risks of personal hosts or servers. For this reason, the Open Web Application Security Project (OWASP) organisation specifically defined the top 10 vulnerabilities, which are the most likely to occur and the most common and dangerous web applications [6]. How to realise the dynamic and active defence of the network has become a research hotspot. Guo et al. [7] studied honeynet technology and provided specific implementations to achieve a more effective security defence. Mohamed et al. [8] studied the security of infinite sensor networks based on an evolutionary game and established a prevention mechanism. Moreover, an active defence model was proposed, and experiments demonstrated that the method effectively improved network reliability and stability. Almohri et al. [9] designed a probabilistic graphical model and linear programming techniques, which were adopted to reduce the possibility of attacks on complex networks, and finally, the reliability of the algorithm was verified by large-scale network experiments. Li et al. [10] designed a malicious code immune program based on an unbalanced support vector machine that enabled proactive defence against malware and maintained the stability of the system. At present, a great deal of research has been conducted only unilaterally by both the attacker and the defender. For example, when considering the attacker, path discovery under both deterministic and non-deterministic conditions is conducted unilaterally from the attacker's perspective, without considering the defence strategy adopted by the defender and its impact on attack path discovery. However, in the actual penetration testing process, there is often a game between the attacker and the defender. Therefore, it is important to study path

planning under the conditions of attack and defence games to improve the automation of penetration testing and realise active network defence.

At present, the effectiveness of web vulnerability defence methods depends on the developer's self-coding security awareness, but penetration tests can enhance the security of the network system as an efficient supplementary means. The penetration process requires testers to conduct continuous black-box or white-box testing to find available attack paths. Nevertheless, numerous redundant processes in penetration testing consume unnecessary time and energy. It is often costly to identify certain available attack paths. System maintainers, or defenders, must expend significant effort to avoid exploitable web vulnerabilities generated by network systems. They also must continuously improve their system's self-protection capabilities to reduce the occurrence of network attacks. Through penetration testing, system defenders can discover dangerous vulnerabilities in the system before a malicious network attack occurs to conduct effective security defence in advance to prevent the attack.

Therefore, at this stage, there is an urgent need for new models or methods that not only allow penetration testers to better discover attack paths in terms of web vulnerabilities but also allow system defenders to reliably predict and analyse the security of their network systems. Simultaneously, defenders can deduce the best defence strategy under the given conditions. The penetration tester and the system defender essentially simulate the attack-defence process of the network in real life, and they derive their benefits from different decisions. To some extent, the process is inseparable from game theory. Therefore, studying the benefits under the conditions of attack-defence games can improve the success rate of penetration testing while significantly helping the defensive side choose its defence strategies.

The rest of the paper is organised as follows. Section 2 describes related work on security testing and attack-defence games. Section 3 describes the web attack-defence game model. Section 4 describes how our model should go for quantitative analysis and obtain the payoff matrix. Section 5 presents algorithms for evaluating web security and Nash equilibria. Section 6 demonstrates the usability of the model through experiments and derives results. Section 7 analyses the experimental results. section 8 concludes with a summary.

2 Related work

In terms of security testing, Shuvalaxmi Dass and Akbar Siami Namin [11] introduced the concept of 'vulnerability coverage', where a given application is adequately tested against a given class of

vulnerabilities reported in the National Vulnerability Database (NVD). The derived idea is to use the Common Vulnerability Scoring System (CVSS) as a means of measuring the fitness of the test inputs generated by the evolutionary algorithm, then identify vulnerabilities that match the generated vulnerability vector through pattern matching, and then test the system under test against these identified vulnerabilities. P.V.R. Murthy et al. [12] argued that existing security coverage standards or test adequacy standards do not have a systematic basis. They proposed that by abstracting functional tests as a sequence of events and mapping events to vulnerabilities as a basis for designing security or penetration tests, and attempt to define test adequacy criteria for web applications. The design of the tests is primarily based on the functional specification of the web application, however, information about potential vulnerabilities in the events can be gathered from different relevant sources, including vulnerable areas of the application code. These concepts are applied to web applications in the banking sector for demonstration purposes. Thanh Binh Dao and Etsuya Shibayama [13] thought that coverage criteria used in traditional software testing such as branch coverage and statement coverage are commonly used but they are not originally defined for security testing purpose. They present an overview of the limitations of those common coverage criteria and propose wrapper coverage, vulnerability-aware sink coverage and vulnerability-aware wrapper coverage as other options that are more appropriate for security testing. These references provide the basis for the modeling and experimental justification of this paper

In recent years, research on network security based on game theory, especially research on network offence and defense, has gradually become more and more widespread. Incomplete information game models are common in real networks. If the attacking and defending parties have accurate knowledge of the process of the game, then it is called a complete information game. Otherwise, it is an incomplete information attacking and defending game [14-16]. Furthermore, if both attackers and defenders have acquiesced and understood the options chosen by both sides before the game, it is called a perfect information game [17,18]. Otherwise, it is called an imperfect information game. Harsanyi proposed a method to deal with incomplete information game models, which had important implications for the study of uncertainty models [19-25]. At present, research on cybersecurity using information game models has made some progress [26]. LYE [27] analysed the interaction strategies of attackers and defenders through a complete information game. Selma et al. [28] proposed a new method of collaborative filtering for recommender systems based on game theory. This

process helped to improve the clustering-based CF process because of the better quality of the user community obtained. Experimental results showed that the proposed method significantly enhanced recommendations. Wang et al. [29] constructed a stochastic evolutionary game model through stochastic differential equations with Markovian properties. Using these stochastic differential equations, the evolutionary equilibrium solution of the model was found, and the stability of the model was proved. The simulation results showed that the stochastic evolutionary game model could obtain a steady state and an optimal defense strategy under the action of stochastic disturbance factors.

The study of game theory gives us the mathematical theory to solve network attack and defence security because mathematical modelling helps us understand the attacker's attack behaviour. Then, the system defender can choose the optimal defence strategy for security protection. Carin [30] proposed a method to quantify cybersecurity risks to improve security strategies and analysed protection strategies for critical infrastructure using the attack and defence models. Lye and Wings [31] used a stochastic game model and analysed the Nash equilibrium of defenders and attackers and their respective optimal strategies [32]. Wang et al. [33] proposed a static Bayesian game active defence strategy selection method, which classified attacker-defenders into various types, considered an attacker-hybrid strategy as a credible prediction of the possible actions of an attacker, calculated the effectiveness of the defence strategy, and gave an optimal active defence strategy selection algorithm. Qian et al. [34] proposed a network defence strategy selection method based on a random game and taboo search. They emphasised that the network defence strategy was the key factor determining the network security protection effectiveness, and they constructed a taboo random game model based on finite rational pre-conditions. Data-driven memory was used in combination with the game model to derive the optimal defence strategy. Sun et al. [35] used Pareto optimisation to design a network attack model method based on a multi-objective game and then designed an optimal attack defence strategy. Mishra et al. [36] proposed an economic optimization model based on game theory that provided insights into optimal configuration of IDS. The innovation was that the strategic interaction between the IDS, the enterprise and the hacker should be incorporated when determining the optimal configuration and algorithm. By incorporating game theory, their contribution was not the particular algorithm used by the IDS, but the game theory and cost analysis principles that determined the optimal configuration of the IDS. Attiah et al. [37] proposed a dynamic game theory framework that predicted the effectiveness of opponent strategies by modelling both offence and defence, and they selected effective defence

strategies through Nash equilibrium analysis. A Nash equilibrium is a solution to a game where none of the players is sufficiently incentivised to change the strategy [38]. Simply put, it is a state in which each player will continue doing what it has been doing [39].

The literature analysis above shows that, based on the existing network offensive and defensive game models, certain research results have been achieved in network risk prediction and the selection of optimal defence paths. Some of these model methods have been applied to corporate networks or military fields, which play a necessary role. As web technology has been widely promoted and applied on networks, network attacks exploiting web vulnerabilities have become increasingly severe. However, existing research on network offence and defence based on game theory only considers inclusive strategies, the research on web vulnerabilities based on game theory is still in a vacant state, no model has mentioned specific quantification and division of exploitable vulnerabilities, and attack-defence benefits are not calculated correctly. The consideration of factors in the actual offensive and defensive process is not sufficiently combined with the network offence and defence. Therefore, because of the previous deficiencies, this paper focuses on web vulnerabilities based on game theory. The top 10 web vulnerabilities listed by OWASP are specifically categorised, and the parameters are quantified. When calculating the benefits, the cost of making decisions by both offensive and defensive parties is fully considered. In attacking and defending against vulnerabilities, the 'ability difference' is introduced to measure the differences in the abilities of the offensive and defensive parties to select strategies. We also discuss the difficulty of vulnerability exploitation and detection, the influence of vulnerability hazards, and the prevalence of vulnerabilities in the attack-defence process based on web vulnerabilities. Finally, through the specific quantification of the benefits of both attackers and defenders, the payoff matrix can be deduced for penetration testers to improve the success rate of penetration testing, and system defenders can analyse the actual network situation and accurately choose the corresponding defence strategy to deal with the next malicious attack as well.

3 Establishment of the model

3.1 Basic assumptions of the model

When the offensive and defensive parties engage in cyber confrontation, neither party can clearly grasp the other's decision-making methods because of their different technologies, their different experience, and the objective complexity of cyberspace. Thus, the web network attack and defence confrontation is a game with incomplete information. The following three assumptions must be met for the web attack

and defence model to work.

Assumption 1: Both sides, attacking and defensive, make every decision for their own benefit, they do not invest a significant cost for their own benefit, and they make no decision that is not good for them.

Assumption 2: Both the attacker and the defender have their own goals: the attacker tries to obtain access to information or resources, and the defender tries to prevent their information and resources from being stolen. The gain for both the attacker and the defender can be measured by the important economic value of the information or resources. The attacker's gain is the defender's loss, and they are mutually reinforcing. However, the utility values of the attackers and defenders are not precisely equal due to the different costs of their respective decisions, so the game is a non-zero-sum game.

Assumption 3: Both attackers and defenders have various types of attacks or defences, and both the attacker and the defender choose their own appropriate decision-making strategies among the identified types.

3.2 Design of the model

The actual network attack-defence confrontation process can be fully simulated by the web attack-defence game model (WADG). The WADG can be defined as a five-tuple array model $G_{WADG}=\{N, T, A, C, U\}$, where:

(1) $N=\{N_1, N_2, N_3, \mathrm{L}, N_n\}$ is the set of participants in the attack-defence game. The number of participants in the game is n. In this paper, the network attacker and the defender are each regarded as single participants, so n=2 and the participants in the game model N can be written as $N=\{N_A, N_D\}$.

(2) $T=\{T_1, T_2, \mathrm{L}, T_n\}$ represents the set of web application security risk types. In addition, $T_A=\{T_1^A, T_2^A, \mathrm{L}, T_n^A\}$ is the set of attack types of the network attackers and $T_D=\{T_1^D, T_2^D, \mathrm{L}, T_n^D\}$ is the set of defence types of the network defenders. For example, when drawing from the 10 most serious web application security risks defined by OWASP, $1 \le n \le 10$.

(3) $A=\{A_1, A_2, \mathrm{L}, A_n\}$ represents the set of attack-defence strategies of the game participants, with $A_A=\{A_1^A, A_2^A, \mathrm{L}, A_e^A\}$ as the set of the attacker's strategies and $A_D=\{A_1^D, A_2^D, \mathrm{L}, A_f^D\}$ as the set of the defender's strategies, where $e \in Z_+$, $f \in Z_+$, $e+f=n$, and $n \in Z_+$.

(4) $C=\{C_1,C_2,\mathrm{L}\ ,C_n\}$ represents the set of the game participants' costs for the attack-defence strategy, with $C_A=\{C_1^A,C_2^A,\mathrm{L}\ ,C_e^A\}$ as the set of the attacker's attack costs and $C_D=\{C_1^D,C_2^D,\mathrm{L}\ ,C_f^D\}$ as the set of the defender's costs, where $e\in Z_+$, $f\in Z_+$, $e+f=n$, and $n\in Z_+$.

(5) $U=\{U_1,U_2,\mathrm{L}\ ,U_n\}$ represents the set of payoff matrixes of the game participants. In this paper, where the network attacker is regarded as a single participant and the network defender is regarded as a single participant, making n=2, the set of the game participants' income in the game model U can be written as $U=\{U_A,U_D\}$. Taking web vulnerabilities as an example, $U_A(T_i^A,A_e^A,A_f^D,C_e^A)$ is the attacker's payoff matrix, where the attacker uses a vulnerability type defined by OWASP as T_i^A, the attacker's attack strategy is A_e^A, the defender's defence strategy is A_f^D, and the attacker's attack cost is C_e^A. Simultaneously, $U_D(T_j^D,A_f^D,A_e^A,C_f^D)$ expresses the defender's payoff matrix, where the defender selects the defence type T_j^D based on the vulnerability type, the defender's defensive strategy is A_f^D, the attacker's attack strategy is A_e^A, and the defender's cost is C_f^D, where $\forall A_e^A\in A_A$, $A_f^D\in A_D$, $T_i^A\in T_A$, $T_j^D\in T_D$, $C_m^A\in C_A$, and $C_n^D\in C_D$.

4. Methodology for quantifying gains on the network attack-defense game

In the network attack-defence game, both sides choose different strategies at various stages based on their respective profitability. Thus, to a certain extent, how closely the quantification of the strategic profitability approaches the actual situation directly affects the success rate of penetration testing. For system maintainers, this can directly affect whether the network system is secure. Therefore, this section quantifies the gains of both attackers and defenders based on penetration testing or the actual process of attack-defence.

4.1 The quantitative basis of attack-defence gains

In a cyber attack and defence game, both rational attackers and defenders choose their actions based on the payoffs of their strategies. Therefore, whether the quantification of the benefits of a strategy is reasonable directly affects the results of cyber security risk assessment accuracy. As network attack and

defence strategies are composed of different attack and defence actions in the process of quantifying the benefits of cyber attack and defence, the benefits of a particular action in the strategy are firstly the benefits of a particular action in the strategy, and then quantify the benefits of the strategy as a whole. The benefits of the strategy as a whole are then quantified.

Definition 1: Network system value. This is the measure of the damage to the security of the network, comprising integrity, confidentiality, and usability values. We use $R = (R(\mathrm{K}_1), R(\mathrm{K}_2), R(\mathrm{K}_3))$ to represent the value, where $R(\mathrm{K}_1), R(\mathrm{K}_2), R(\mathrm{K}_3)$ are the integrity, confidentiality, and availability values, respectively.

Definition 2: Difficulty of exploiting the vulnerability. This is the measure of the difficulty for penetration testers to exploit various types of vulnerabilities. We use $D = (D_1, D_2, D_3)$ to represent the difficulty, where D_1, D_2, D_3 represent easy, moderate, and difficult, respectively.

Definition 3: Impact of the vulnerability. This reflects the damage to the host system from various types of vulnerabilities. We use $V = (V_1, V_2, V_3)$ to represent the impact of the vulnerability, where V_1, V_2, V_3 represent light, moderate, and severe damage, respectively.

Definition 4: Difficulty in detecting the vulnerability. This reflects the ease of exploitation or discovery of vulnerabilities for both attackers and defenders. We use $O = (O_1, O_2, O_3)$ to represent the difficulty of detecting the vulnerability, where O_1, O_2, O_3 represent easy, moderate, and difficult detection, respectively.

Definition 5: Prevalence of vulnerabilities. This reflects the proficiency of penetration testers in exploiting vulnerabilities, which directly affects penetration testers' selection of vulnerability types, which in turn affects the entire decision-making process. We use $L = (L_1, L_2, L_3)$ to represent the prevalence of vulnerabilities, where L_1, L_2, L_3 represent widespread, common, and uncommon vulnerabilities, respectively.

Definition 6: Probability of successful penetration. This is the probability that the penetration tester successfully enters the defender's network system by exploiting a certain type of vulnerability. We use α to represent this probability. For the defender, the defence process includes both the probability of successfully detecting an attack and the probability of successfully defending against it. We express this as ω, γ, so the probability of successful penetration is α=1-ω*γ.

Definition 7: Penetration gains. This reflects the benefits that a penetration tester can gain from the penetration. They are measured by the damage caused to a network system, including direct and indirect gains. Indirect gain refers to cases where the defender's system was not successfully breached, but the attack process provided information about the defender's defences or other important information about the system. Direct gain refers to the damage caused to the network system by successfully breaching the defender's system through certain vulnerabilities to achieve the attacker's ultimate goal. In this model, we introduce a reducing factor λ for indirect gains to quantify the degree of damage to the system [40].

Definition 8: Defence gains. This reflects the gains obtained by system defenders from their defence, that is, the quantitative value of protecting the network system from loss or the defence gains obtained by protecting the network system from attacks.

4.2 Quantitative calculation of attack- defense gains

During penetration testing, the type of OWASP vulnerability selected by the penetration tester is T_i^A, the penetration strategy is A_e^A, and the penetration cost is C_e^A. The system defender selects defence type T_j^D based on the type of OWASP vulnerability, the defensive strategy is A_f^D, and the defence cost is C_f^D. The probability that the defender detects the attack through its own defence system is ω_e, and the probability of successful defence is γ_f.

For penetration testers, the security attributes of penetration testing are K_z. The direct mathematical expectation can be quantified by formula (1):

$$E_{(1)}(K_z) = \alpha_{ef} * [T_i^A(L)] * [T_i^A(V)] * (R(K_1) + R(K_2) + R(K_3)) \quad (1)$$

where α_{ef} is the probability of successful penetration, $T_i^A(L)$ is the prevalence of vulnerability T_i^A, $T_i^A(V)$ is the impact of vulnerability T_i^A, and $R(*)$ represents the integrity, confidentiality, and usability values. Similarly, the indirect mathematical expectation can be quantified by the formula (2):

$$E_{(2)}(K_z) = \lambda_e * \omega_e * \gamma_f * [T_i^A(L)] * [T_i^A(V)] * (R(K_1) + R(K_2) + R(K_3)) \quad (2)$$

where λ_e is the reducing factor.

When the type of vulnerability is T_i^A and the penetration strategy is A_e^A, the total penetration

cost is $F(T_i^A(A_e^A))$. This is quantified by formula (3):

$$F(T_i^A(A_e^A)) = C_e^A * [T_i^A(D)] * [T_i^A(O)] \tag{3}$$

where $T_i^A(D)$ is the difficulty of exploiting vulnerability T_i^A and $T_i^A(O)$ is the difficulty of detecting vulnerability T_i^A.

Through the above analysis, it can be concluded that when the type of OWASP vulnerability selected by the penetration tester is T_i^A and the penetration strategy is A_e^A, the gain for the penetration can be quantified by formula (4):

$$U_A(T_i^A, T_j^D, A_e^A, A_f^D, C_e^A) = (\lambda_e * \omega_e * \gamma_f + \alpha_{ef}) * [T_i^A(L)] * [T_i^A(V)] * (R(K_1) + R(K_2) + R(K_3)) - C_e^A * [T_i^A(D)] * [T_i^A(O)] \tag{4}$$

When the system defender selects defence type T_j^D, the defensive strategy is A_f^D. In the same way, the benefit of the defender can be quantified by formula (5):

$$U_D(T_i^A, T_j^D, A_e^A, A_f^D, C_f^D) = \omega_e * \gamma_f * [T_i^A(L)] * [T_i^A(V)] * (R(K_1) + R(K_2) + R(K_3)) - C_f^D * [T_i^A(O)] \tag{5}$$

4.3 Difference in Capabilities

In our actual network attack-defence confrontation, the attacking and defending sides do not make only one decision per round, like a chess game, because the capabilities, experience, and information processing speed of the attacking and defending sides are different. Therefore, in the actual network confrontation, the side with the superior information processing ability often has a significant advantage and can implement multiple strategies or multiple groups of strategies during one round. In response to this problem, Wang et al. [30] proposed the concept of astringency to quantify the difference in strategy selection capabilities between attackers and defenders. We use the concept of astringency in this paper for different vulnerability types and processing capabilities.

The ability difference quantifies the difference in strategy selection ability between attackers and defenders, represented by $\psi_{ij} = [\frac{\mathrm{M}(T_i^A)}{\mathrm{M}(T_j^D)}]$, where $\mathrm{M}(T_i^A)$ is the penetration tester's ability to use vulnerability type T_i^A and $\mathrm{M}(T_j^D)$ is the system defender's ability to handle vulnerability type T_j^D. The vulnerability handling ability of both sides can be quantified by a positive integer less than 10, and the ratio of the attacker's and defender's vulnerability handling ability is rounded up.

The difference in vulnerability handling ability between the attacker and defender changes the gains in an attack-defence cycle, thus affecting the whole network attack-defence game model. When

the attacker has an information advantage, the defender implements a strategy for a period of time, and the attacker can implement a set of strategies. In the specific quantification process, the attacker must choose an attack strategy that does not consider the difference in capabilities. Moreover, other strategies in the attack strategy set are selected based on equal probabilities. Assuming that the vulnerability type is T_i^A, there are z attack strategies, and $\beta = \frac{1}{z-1}$, the expected gains for the attackers and defenders can be quantified by the following formulas (6) and (7):

$$U'_A(T_i^A, T_j^D, A_e^A, A_f^D, C_e^A) = U_A(T_i^A, T_j^D, A_e^A, A_f^D, C_e^A) + (\psi_{ij} - 1)\sum_{\substack{h=1 \\ h \neq e}} \beta U_A(T_i^A, T_j^D, A_h^A, A_f^D, C_h^A) \quad (6)$$

$$U'_D(T_i^A, T_j^D, A_e^A, A_f^D, C_f^D) = U_D(T_i^A, T_j^D, A_e^A, A_f^D, C_f^D) - (\psi_{ij} - 1)\sum_{\substack{h=1 \\ h \neq e}} \beta U_A(T_i^A, T_j^D, A_h^A, A_f^D, C_h^A) \quad (7)$$

When the penetration tester and the system defender use different types of OWASP attack-defence methods to conduct attack-defence games, the total revenue of both sides can be quantified by the following formulas (8) and (9):

$$u_A(\text{sum}) = \sum_{i=1}^{10}\sum_{e=1}^{z}\sum_{f=1}^{x} U'_A(T_i^A, T_j^D, A_e^A, A_f^D, C_e^A) \quad \text{among them } i = j \quad (8)$$

$$u_D(\text{sum}) = \sum_{j=1}^{10}\sum_{e=1}^{z}\sum_{f=1}^{x} U'_D(T_i^A, T_j^D, A_e^A, A_f^D, C_f^D) \quad \text{among them } i = j \quad (9)$$

4.4 Equilibrium analysis of the game

(1) Hybrid strategy:

In the WADG model, the penetration tester chooses a pure attack strategy P_r^A that satisfies $0 \le P_r^A \le 1$ and $\sum_{r=1}^{k} P_r^A = 1$. Then, $P_x^A = \{P_1^A, P_2^A, P_3^A, \text{L}, P_k^A\}$ is a mixed strategy for penetration testers. Likewise, a mixed strategy for the system defender is $P_y^D = \{P_1^D, P_2^D, P_3^D, \text{L}, P_l^D\}$.

(2) Analysis of mixed strategy Nash equilibrium:

Nash used the fixed-point theorem to prove that every limited-strategy game has at least one pure-strategy or mixed-strategy Nash equilibrium [41]. According to this principle, a Nash equilibrium exists in every finite strategy game [11]. During the game, the mixed strategy of the penetration tester is $P_x^A = \{P_1^A, P_2^A, P_3^A, \text{L}, P_k^A\}$, the mixed strategy of the system defender is $P_y^D = \{P_1^D, P_2^D, P_3^D, \text{L}, P_l^D\}$, and the revenue utility at the Nash equilibrium point is $U_A(P_*^A, P_*^D)$,

$U_D(P_*^A, P_*^D)$. A mixed strategy (P_*^A, P_*^D) is a Nash equilibrium only if the following equations (10) and (11) are satisfied:

$$\forall x \in [1,k] \qquad U_A(P_*^A, P_*^D) \geq U_A(P_x^A, P_*^D) \tag{10}$$

$$\forall y \in [1,l] \qquad U_D(P_*^A, P_*^D) \geq U_D(P_*^A, P_y^D) \tag{11}$$

5 Network security risk assessment based on offensive and defensive games

Web security risks are assessed by analyzing the likelihood of web security problems occurring and the consequences after they occur. In the web attack and defense game model, based on quantifying the benefits of attack and defense strategies, the mixed strategy Nash equilibrium (P_*^A, P_*^D) can be obtained through game equilibrium analysis. Mixed strategy Nash equilibrium P_*^A is the probability of web security threats occurring. Penetration tester's gain function $\mathrm{u}_A(\mathrm{sum})$ is the loss to the network caused by the attack, i.e., the consequences of the security problem after it occurs. On the basis of web attack and defense game model determination, the evaluation formula of network security risk is:

$$\mathrm{Result} = \sum_{i=1}^{10}\sum_{e=1}^{z}\sum_{f=1}^{x} P_{\mathrm{i}}^A \frac{U'_A(T_i^A, T_j^D, A_e^A, A_f^D, C_e^A)}{\max\left(U_A\left(A_A, A_D\right)\right)} \tag{12}$$

5.1 Risk assessment algorithm

The web offensive and defensive game is a finite strategy game. Nash used Brouwer's immobility point theorem to prove that every finite strategy game has at least one Nash equilibrium. Therefore, the web attack and defense game model must be able to predict the web attack behavior. The algorithm of web security risk assessment based on attack and defense game is shown below.

Algorithm 1: Network security risk assessment algorithm based on offensive and defensive games.

Input: Network Attack and Defense Game Model (WADG).

Output: Result of the cyber security risk assessment (Result).

a) Initialization of the web attack and defense game model $G_{WADG} = \left(\left(N_A, N_D\right), \left(T_A, T_D\right), \left(A_A, A_D\right), \left(C_A, C_D\right), \left(U_A, U_D\right)\right)$

b) Construct the set of attack and defence types for both sides $T_A = \left(T_1^A, T_2^A, \mathrm{L}\ , T_n^A\right)$, $T_D = \left(T_1^D, T_2^D, \mathrm{L}\ , T_n^D\right)$

c) Build a collection of offensive and defensive strategies for both sides $A_A = \left(A_1^A, A_2^A, \mathrm{L}\ , A_e^A\right)$, $A_D = \left(A_1^D, A_2^D, \mathrm{L}\ , A_f^D\right)$

d) Constructing a collection of offensive and defensive costs for both sides $C_A=\left(C_1^A,C_2^A,\mathrm{L}\ ,C_e^A\right)$, $C_D=\left(C_1^D,C_2^D,\mathrm{L}\ ,C_f^D\right)$

e) Calculation of penetration tester gains by equation (4) and equations (6) and (8) $\mathrm{u}_A(\mathrm{sum})$

f) Calculation of system defender gains by equation (5) and equations (7) and (9) $\mathrm{u}_D(\mathrm{sum})$

g) The returns of both sides of the hybrid strategy are calculated by equations (10) and (11), and the return matrix U_A, U_D is generated.

h) Calling the mixed strategy Nash equilibrium solution sub-algorithm Slove(WADG).

i) Based on the determination of the Nash equilibrium and the payoff matrix, the web security risk is quantified by equation (12).

j) Get the web security risk assessment value Result

Algorithm 2: Mixed strategy Nash equilibrium solution sub-algorithm Slove(WADG).

Input: web offensive and defensive game model WADG.

Output: mixed strategy Nash equilibrium.

a) Initialization of the web attack and defense game model $G_{WADG}=\left(\left(N_A,N_D\right),\left(T_A,T_D\right),\left(A_A,A_D\right),\left(C_A,C_D\right),\left(U_A,U_D\right)\right)$

b) Constructing the gain matrix U_A,U_D for both attackers and defenders.

c) Solve the following nonlinear program:

$$arg\ max f\left(T_A,T_D,A_A,A_D,C_A,C_D,U_A,U_D\right)=\sum_{i=1}^{10}\sum_{e=1}^{z}\sum_{f=1}^{x}P_e^AP_f^DU'_A(T_i^A,T_j^D,A_e^A,A_f^D,C_e^A)+\sum_{i=1}^{10}\sum_{f=1}^{x}\sum_{e=1}^{z}P_f^DP_e^AU'_D(T_i^A,T_j^D,A_e^A,A_f^D,C_f^D)-v_1-v_2$$

$$s.t.\sum_{i=1}^{10}\sum_{f=1}^{x}P_f^DU'_A(T_i^A,T_j^D,A_e^A,A_f^D,C_f^D)\le v_1\ ;\ e=1,2,3,\mathrm{L}\ ,z$$

$$\sum_{i=1}^{10}\sum_{\mathrm{e}=1}^{z}P_{\mathrm{e}}^AU'_A(T_i^A,T_j^D,A_e^A,A_f^D,C_{\mathrm{e}}^A)\le v_2\cdot\ \ f=1,2,3,\mathrm{L}\ ,x$$

$P_f^D\in[0,1]$, $P_{\mathrm{e}}^A\in[0,1]$ $\sum_{f=1}^{x}P_f^D=1$, $\sum_{\mathrm{e}=1}^{z}P_{\mathrm{e}}^A=1$, and a mixed strategy Nash equilibrium can be obtained.

6 Experiment

To verify that the game model in this paper, based on the common vulnerabilities listed by OWASP, not only allows penetration testers to better discover effective attack strategies based on web vulnerabilities but also allows system maintainers to reliably predict and analyse the security of their

own network systems before they are threatened, the following network environment was designed for experiments.

Table 1 summarises the top 10 application security risk factors listed in the latest OWASP summary, along with the risk value assigned to each risk factor.

Table 1. Summary of TOP 10 risk factors

Risk	Exploitability	Prevalence	Detectability	Technical impacts	Score
Injection	Easy:3	Common:2	Easy:3	Serious:3	8.0
Broken Authentication.	Easy:3	Common:2	Average:2	Serious:3	7.0
Sensitive Data Exposure.	Average:2	Widely:3	Average:2	Serious:3	7.0
XML External Entities (XXE).	Average:2	Common:2	Easy:3	Serious:3	7.0
Broken Access Control	Average:2	Common:2	Average:2	Serious:3	6.0
Security Misconfiguration.	Easy:3	Widely:3	Easy:3	Medium:2	6.0
Cross-Site Scripting (XSS)	Easy:3	Widely:3	Easy:3	Medium:2	6.0
Insecure Deserialization	Difficult:1	Common:2	Average:2	Serious:3	5.0
Using Components with Known Vulnerabilities	Average:2	Widely:3	Average:2	Medium:2	4.7
Insufficient Logging & Monitoring.	Average:2	Widely:3	Difficult:1	Medium:2	4.0

According to the method proposed in this paper, the set of three common attack strategies for the penetration tester testing the system based on the top 10 types of vulnerabilities is shown in **Table 2**.

Table 2. A set of common attack strategies based on different types

Type name	Attack strategy
Injection	SQL injection (A1)
	OS injection (A2)
	Cookie injection (A3)
Broken Authentication	Permits default, weak, or well-known passwords (A4)
	Exposes Session IDs in the URL (A5)
	Uses plain text, encrypted, or weakly hashed passwords (A6)
Sensitive Data Exposure	Steals plaintext data (A7)

	Steals the encryption key (A8)
	Monitor network traffic (A9)
	Accepts XML directly or XML uploads (A10)
XML External Entities (XXE).	Inserts untrusted data into XML documents (A11)
	Billion Laughs (A12)
	Bypassing access control checks by modifying the URL, internal application state, or the HTML page (A13)
Broken Access Control	Permitting viewing or editing someone else's account (A14)
	Replaying or tampering with a JSON Web Token (JWT)access control token or a cookie (A15)
	Unnecessary features are enabled or installed (A16)
Security Misconfiguration.	Default accounts and their passwords still enabled and unchanged (A17)
	Error handling reveals stack traces or other overly informative error messages to users(A18)
	MFA bypass (A19)
Cross-Site Scripting (XSS)	Session stealing (A20)
	DOM node replacement (A21)
	Achieves arbitrary remote code execution (A22)
Insecure Deserialization	Data tampering attack (A23)
	Access-control-related attacks (A24)
	CVE-2017-5638 (A25)
Using Components with Known Vulnerabilities	Applications and APIs using components with known vulnerabilities (A26)
	Coding error (A27)
	Insufficient logging and monitoring (A28)
Insufficient Logging & Monitoring	Allows attackers to further attack systems, maintain persistence (A29)
	Application is unable to detect attacks (A30)

The set of three common defence strategies for the system defender based on the top 10 types of vulnerabilities is shown in **Table 3**.

Table 3 A set of common defense strategies based on different types

Type name	Defense strategy
Injection	Use a safe API (D1)
	Filter user’s input (D2)

	Use positive or "whitelist" server-side input validation. (D3)
	Multi-factor authentication (D4)
Broken Authentication.	Implement weak-password checks (D5)
	Limit or increasingly delay failed login attempt (D6)
	Classify data processed, stored, or transmitted by an application (D7)
Sensitive Data Exposure	Use the latest and strong standard algorithm or password (D8)
	Ensure up-to-date and strong standard algorithms, protocols, and keys are in place (D9)
	Avoiding serialization of sensitive data (D10)
XML External Entities (XXE)	Patch or upgrade all XML processors and libraries in use by the application or on the underlying operating system (D11) Verify that XML or XSL file upload functionality validates incoming XML using XSD validation or similar (D12)
	With the exception of public resources, deny by default (D13)
Broken Access Control	Implement access control mechanisms once and reuse them throughout the application (D14)
	JWT tokens should be invalidated on the server after logout (D15)
	A minimal platform without any unnecessary features, components, documentation, and samples (D16)
Security Misconfiguration	Sending security directives to clients (D17)
	A task to review and update the configurations appropriate to all security notes, updates and patches as part of the patch management process (D18)
	Drop all untrusted HTTP request data (D19)
Cross-Site Scripting (XSS)	Applying context-sensitive encoding (D20)
	Enabling a Content Security Policy (CSP) (D21)
	Implementing integrity checks (D22)
Insecure Deserialization	Enforcing strict type constraints during deserialization (D23)
	Logging deserialization exceptions and failure (D24)
	Remove unused dependencies, unnecessary features, components, files, and documentation(D25)
Using Components with Known Vulnerabilities	Obtain components from official sources over secure links (D26)
	Continuously monitor sources like CVE and NVD for vulnerabilities in the components. (D27)
Insufficient Logging & Monitoring	Ensure all login, access control failures, and server-side input validation failures can be logged with sufficient user context to identify suspicious or malicious accounts, and held for sufficient time to allow delayed forensic analysis. (D28)
	Establish effective monitoring and alerting (D29)
	Establish or adopt an incident response and recovery plan (D30)

Parameters were developed using statistics from this experiment and the detailed descriptions of the related vulnerabilities by the Common Vulnerability Scoring System, combined with the opinions of network security experts. The parameters relevant to the penetration action are shown in **Table 4**, the parameters relevant to the system defence cost are shown in **Table 5**, and the parameters relevant to the system defence success probability are shown in **Table 6**.

Table 4 Parameters of Penetration Testing

Strategy	λ	ω_e	C_e^A
A1	0.3	0.8	10
A2	0.3	0.8	20
A3	0.2	0.7	10
A4	0.3	0.8	20
A5	0.2	0.7	10
A6	0.3	0.8	20
A7	0.2	0.8	20
A8	0.2	0.7	30
A9	0.3	0.7	30
A10	0.2	0.8	20
A11	0.2	0.8	30
A12	0.2	0.7	30
A13	0.3	0.7	30
A14	0.2	0.7	20
A15	0.2	0.8	30
A16	0.2	0.6	20
A17	0.1	0.8	10
A18	0.2	0.8	20
A19	0.1	0.7	20
A20	0.1	0.7	20
A21	0.2	0.7	20
A22	0.3	0.8	20

A23	0.2	0.6	20
A24	0.2	0.6	20
A25	0.1	0.6	20
A26	0.2	0.7	30
A27	0.2	0.6	20
A28	0.1	0.5	20
A29	0.1	0.5	10
A30	0.2	0.5	20

Table 5 Parameters of system defense cost

Strategy	ω_e	C_f^D
D1	0.8	10
D2	0.8	10
D3	0.7	20
D4	0.8	30
D5	0.7	10
D6	0.8	10
D7	0.8	30
D8	0.7	20
D9	0.7	20
D10	0.8	10
D11	0.8	20
D12	0.7	10
D13	0.7	30
D14	0.7	20
D15	0.8	20
D16	0.6	20
D17	0.8	20
D18	0.8	30
D19	0.7	20

D20	0.7	20
D21	0.7	20
D22	0.8	10
D23	0.6	30
D24	0.6	20
D25	0.6	10
D26	0.7	20
D27	0.6	20
D28	0.5	10
D29	0.5	20
D30	0.5	30

Table 6 Parameters of system defense related actions

(1) Injection

γ	D1	D2	D3
A1	0.8	0.7	0.9
A2	0.8	0.7	0.9
A3	0.7	0.6	0.9

(2) Broken Authentication

γ	D4	D5	D6
A4	0.7	0.8	0.2
A5	0.1	0.1	0.9
A6	0.2	0.9	0.1

(3) Sensitive Data Exposure

γ	D7	D8	D9
A7	0.6	0.8	0.9
A8	0.4	0.9	0.6
A9	0.8	0.8	0.8

(4) XML External Entities (XXE).

γ	D10	D11	D12
A10	0.7	0.6	0.8.
A11	0.8	0.5	0.6
A12	0.8	0.9	0.5

(5) Broken Access Control

γ	D13	D14	D15
A13	0.9	0.4	0.1
A14	0.8	0.6	0.1
A15	0.7	0.3	0.9

(6) Security Misconfiguration

γ	D16	D17	D18
A16	0.5	0.8	0.7
A17	0.6	0.4	0.9
A18	0.8	0.3	0.8

(7) Cross-Site Scripting (XSS)

γ	D19	D20	D21
A19	0.7	0.8	0.9
A20	0.6	0.8	0.9
A21	0.7	0.7	0.9

(8) Insecure Deserialization

γ	D22	D23	D24
A22	0.2	0.7	0.7
A23	0.8	0.6	0.7
A24	0.8	0.7	0.7

(9) Using Components with Known Vulnerabilities

γ	D25	D26	D27
A25	0.2	0.1	0.9
A26	0.3	0.8	0.9
A27	0.5	0.8	0.9

(10) Insufficient Logging & Monitoring

γ	D28	D29	D30
A28	0.3	0.9	0.7
A29	0.8	0.8	0.8
A30	0.8	0.9	0.8

In our experiment, the value of the average security attributes of the network system was specified as (20, 21, 22). The penetration tester selected three mixed strategies, (A1, A4, A7, A10, A13, A16, A19, A22, A25, A28), (A2, A5, A8, A11, A14, A17, A20, A23, A26, A29), and (A3, A6, A9, A12, A15, A18, A21, A24, A27, A30), from the penetration methods based on the various web vulnerability types. The system defender also selects three mixed-defence strategies, (D1, D4, D7, D10, D13, D16, D19, D22, D25, D28), (D2, D5, D8, D11, D14, D17, D20, D23, D26, D29), and (D3, D6, D9, D12, D15, D18, D21, D24, D27, D30). Using formulas (1)-(9), we can calculate the respective payoff matrices of both parties, U_A, U_D, as follows.

$$U_A = \begin{bmatrix} 198.66 & 189.82 & 269.27 & 168.66 & 91.30 & 267.28 & 191.30 & 47.84 & 184.78 & 157.98 \\ 209.82 & 336.83 & 161.23 & 197.04 & 170.99 & 259.14 & 167.49 & 14.57 & 79.10 & 131.28 \\ 177.49 & 316.83 & 224.74 & 212.16 & 40.27 & 164.47 & 167.49 & 5.50 & 103.14 & 111.36 \end{bmatrix}$$

$$U_D = \begin{bmatrix} 231.92 & 151.67 & 198.14 & 201.68 & 232.16 & 93.40 & 165.22 & 10.24 & 10.24 & 8.40 \\ 201.68 & 6.46 & 388.24 & 131.20 & 118.76 & 100.96 & 191.68 & 8.04 & 101.12 & 35.60 \\ 218.14 & 10.24 & 322.88 & 122.30 & 232.16 & 211.92 & 218.14 & 39.38 & 96.08 & 15.60 \end{bmatrix}$$

When considering the differences in capabilities, the ability of the penetration tester using various types of vulnerabilities is categorised according to the difficulty of exploiting the vulnerability newly defined by OWASP. The difference in capabilities can be represented as $\psi_{ij} = [\frac{\mathrm{M}(T_i^A)}{\mathrm{M}(T_j^D)}]$, where $1 \le \psi \le 3$. Specific values are shown in **Table 7.**

In the actual attack-defence process, the two sides form a strong confrontational relationship, and it is difficult for both sides to predict each other's decision in advance.[38] Therefore, the penetration tester randomly selects three mixed strategies based on different penetration methods.

Table 7 The Value of ψ under different types

OWASP type	ψ
Injection	3
Broken Authentication.	3
Sensitive Data Exposure	2
XML external entities	2
XML External Entities (XXE)	2
Broken Access Control	3
Security Misconfiguration	3
Cross-Site Scripting (XSS)	1
Insecure Deserialization	2
Using Components with Known Vulnerabilities	2

(A1A2A3, A4A5A6, A7A8, A10A11, A13A14, A16A17A18, A19A20A21, A22, A25A26, A28A29)

(A1A2A3, A4A5A6, A8A9, A11A12, A14A15, A16A17A18, A19A20A21, A23, A26A27, A29A30)

(A1A2A3, A4A5A6, A7A9, A10A12, A13A15, A16A17A18, A19A20A21, A24, A25A27, A28A30)

The system defender selects three mixed-defence strategies, (D1, D4, D7, D10, D13, D16, D19, D22, D25, D28), (D2, D5, D8, D11, D14, D17, D20, D23, D26, D29), and (D3, D6, D9, D12, D15, D18, D21, D24, D27, D30). Using formulas (1)-(9), we can calculate the respective payoff matrices of both sides, U_A, U_D, as follows.

$$U_A=\begin{bmatrix} 607.14 & 822.34 & 429.27 & 230.89 & 146.21 & 636.45 & 616.24 & 47.84 & 259.62 & 217.95 \\ 670.64 & 652.97 & 273.6 & 260.79 & 263.70 & 694.84 & 544.80 & 14.57 & 136.72 & 196.92 \\ 522.46 & 779.98 & 304.95 & 284.39 & 160.01 & 476.18 & 454.84 & 5.50 & 147.90 & 162.01 \end{bmatrix}$$

$$U_D = \begin{bmatrix} -176.56 & -480.85 & 38.14 & 139.45 & 177.25 & -275.77 & -259.72 & 10.24 & -64.6 & -51.57 \\ -259.14 & -309.68 & 275.87 & 67.45 & 26.05 & -334.74 & -185.63 & 8.04 & 43.5 & -30.04 \\ -126.83 & -452.91 & 242.67 & 50.07 & 112.42 & -99.79 & -69.21 & 39.38 & 51.32 & -35.05 \end{bmatrix}$$

According to the Nash equilibrium principle, every limited-strategy game has a Nash equilibrium.[35] The theoretical game in this paper is a finite game, so there must be an equilibrium point, which can be obtained through the mixed-strategy Nash equilibrium solution algorithm: penetration testers obtain the greatest benefits from penetration strategies (A1A2A3, A4A5A6, A7A8, A10A11, A13A14, A16A17A18, A19A20A21, A22, A25A26, A28A29). The system defender always secures the system so that the system suffers the least damage and cost. The algorithm calculates the defender's optimal mix of policies, (D3, D6, D9, D12, D15, D18, D21, D24, D27, D30), that will result in the least damage to the system.

The relationships between the penetration gains and cost and the system defender’s gains and cost when considering the difference in capabilities are shown in **Fig.1 and Fig.2.**

From the analysis of **Fig.1** and **Fig.2**, we can conclude that in the penetration testing process, we should fully consider the cost of each step of the decision and the impact of the vulnerability, which may reduce the gains but require a significant cost. In the defence process, system defenders should fully consider the different hazards brought by different web vulnerabilities to the system security attributes and selectively increase the defensive ability and the cost to protect against certain web vulnerabilities, such as injection vulnerabilities, failed authentication vulnerabilities, security configuration errors, and cross-site scripting attacks in this example. In **Fig.1** and **Fig.2**, when the penetration testers have higher gains, the gains of the system defenders decrease and the network security risk increases, which is consistent with the changing trend in actual networks.

Fig.1 and **Fig.2** together show that the more accurate the defender's judgement of the attacker's type, the more appropriate defensive measures can be chosen to counter the attack, thus increasing the defender's gain. The defender's judgement of the attacker's type directly affects the game equilibrium solution and the quantification of defence effectiveness, which in turn affects the choice of defence strategy. Therefore, in practical network security defence, defence strategies and attack detection are deployed together to enhance the effectiveness of network security defence. As can be seen from **Fig.2**, when considering different capabilities, the more resistant the defence strategy selected by the defender is to attack actions, the better it can protect the target device from being breached by the attacker, thus improving the benefits for the defender. When faced with a network attack, the success rate of the

defence is positively correlated with the strength of the defence strategy. Therefore, where network resources allow, high-intensity defensive measures should be adopted to enhance network security defence.

Therefore, the quantification method of attack-defence gains proposed in this paper can effectively enhance the penetration success rate of the penetration testing party, and the system defence party can conduct targeted defence enhancement according to the defence payoff matrix, enhance the amount of information for effective defence, and improve its own defence ability. Thus, the method proposed in this paper can provide effective reference values for both parties in the actual web vulnerability domain.

7 Conclusions

In the process of categorising and quantifying web vulnerabilities, this paper comprehensively considers the difficulty of web vulnerability exploitation and detection and the impact and prevalence of the vulnerabilities in the attack-defence process. The choice of strategies, based on different costs, has an impact on income and the different strategy choices brought about by the different abilities of the two parties, making the calculation of income more in line with real networks. A type of web security assessment and strategy optimisation is proposed based on an attack-defence game using a payoff matrix. In addition, the usability and effectiveness of the model method were verified through a simulation of the attack-defence environment. Based on the payoff matrix, the penetration tester can find the penetration node more accurately through various vulnerability analyses. Meanwhile, the defender can find nodes with potential safety hazards as soon as possible and conduct an effective defence through the value of defence benefits to improve the system defence and detection success rate.The main conclusions reached are as follows:

1) An offensive and defensive game model is constructed based on the characteristics of actual information networks, fully considering the impact of the types, strategies and costs of both attackers and defenders on the game process, making the model more in line with the actual situation of information network confrontation and laying the foundation for the study of active network security defence.

2) The vulnerabilities are considered in detail, which is more in line with the deployment of the strategies of both attackers and defenders in the actual confrontation and is highly relevant.

3) The quantification method of attack and defence gains is designed from the perspective of the

impact of attack and defence actions on the value of the network system, effectively solving the problem of strong subjectivity in quantifying gains in current game models.

The next step will be to use dynamic game theory to model the process of network attack and defense, and to study the problem of selecting the optimal defense strategy for a network under dynamic change conditions. The next step will be to use dynamic game theory to model the network attack and defence process and to study the optimal defence strategy selection problem under dynamic change conditions.

Ethical Approval and Consent to participate

Not applicable.

Human and Animal Ethics

Not applicable.

Consent for publication

Not applicable.

Availability of supporting data

Not applicable.

Conflict of Interests

The authors declare that they have no conflict of interest.

Funding

This work was supported in part by Open Foundation of State key Laboratory of Networking and Switching Technology (Beijing University of Posts and Telecommunications) under Grant SKLNST-2020-1-15, and in part by introduction of talent research start-up fund of Chongqing University of Posts and Telecommunications under Grant E012A2020210.

Author's contributions

Conceptualization, Yu.W.F, Chen.Z.G.; methodology, Yu.W.F; writing—original draft preparation, Yu.W.F; contribution to contents, review and editing, Chen.Z.G.; supervision, Chen.Z.G. All authors have read and agreed to the published version of the manuscript.

Acknowledgements

Thanks to Chongqing University of Posts and Telecommunications and Beijing University of Posts and Telecommunications for their support of this project.

Authors' information

Wenfei Yu[1], Zigang Chen[2,*]

[1] School of Cyberspace Security, Beijing University of Posts and Telecommunications, Beijing 100876 China.

[2] Chongqing Key Laboratory of Cyberspace and Information Security, Chongqing University of Posts and Telecommunications, Chongqing 400065 China.

References

1. Li, J., Huang, J., Tian, L., Wang, J.: Application of New Active Defense Technology in Power Information Network Security. IOP Conference Series: Materials Science and Engineering **750**, 012156 (2020) https://doi.org/10.1088/1757-899x/750/1/012156**.**
2. Zhao, G., Song, J.: Network security model based on active defense and passive defense hybrid strategy. J Intell Fuzzy Syst **39**, 8897-8905, (2020).
3. Lv, Y., Guo, Y., Chen, Q., Cheng, G., Chen, Y.: Active perceptive dynamic scheduling mechanism based on negative feedback. Procedia Comput Sci **131**, 520-524 (2018) https://doi.org/10.1016/j.procs.2018.04.253.
4. Gordon, L., Loeb, M., Lucyshyn, W., Zhou, L.: Externalities and the Magnitude of Cyber Security Underinvestment by Private Sector Firms: A Modification of the Gordon-Loeb Model. J Inf Secur **06**, 24-30 (2015) https://doi.org/10.4236/jis.2015.61003.
5. Beijing Rising Network Security Technology Co. Ltd, '2020 China Cyber Security Report. J Inf Secur Res **7**, 102-109 (2021).

6. Wichers, D., Williams, J.: Owasp top-10 2017. OWASP Foundation (2017).
7. Guo, H., Luo, J., Geng, Q.: A Study on Cyber Defence Honeynet Technology and Configuration Examples. Int J Simul **17**, 26.21-26.24 (2016).
8. Al-Jaoufi, M.A., Liu, Y., Zhang, Z.: An Active Defense Model with Low Power Consumption and Deviation for Wireless Sensor Networks Utilizing Evolutionary Game Theory. Energies **11**, 1281 (2018) https://doi.org/10.3390/en11051281.
9. Almohri, H.M.J., Watson, L.T., Yao, D., Ou, X.: Security Optimization of Dynamic Networks with Probabilistic Graph Modeling and Linear Programming. IEEE Trans Depend Secure **13**, 474-487 (2016) https://doi.org/10.1109/TDSC.2015.2411264.
10. Li, P., Wang, R.: Research on network malicious code immune based on imbalanced support vector machines. Chinese J Electron **24**, 181-186 (2015).
11. Dass, S., Namin, A.S.: Vulnerability coverage for adequacy security testing. Proceedings of the 35th Annual ACM Symposium on Applied Computing (SAC '20), pp. 540-543 (2020).
12. Murthy, P.V.R., Shilpa, R.G.: Vulnerability Coverage Criteria for Security Testing of Web Applications. 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), pp. 489-494 (2018).
13. Dao, T.B., Shibayama, E.: Coverage Criteria for Automatic Security Testing of Web Applications. In Information Systems Security. ICISS 2010. Lecture Notes in Computer Science. S, S. J., & Mathuria, A., Eds.: Springer, Berlin, Heidelberg (2010).
14. Aumann, R.J.: Game Theory. In The New Palgrave Dictionary of Economics, Palgrave Macmillan UK: London, pp 1-40 (2017).
15. Roy, S., Ellis, C., Shiva, S., Dasgupta, D., Shandilya, V., Wu, Q.: A Survey of Game Theory as Applied to Network Security. 2010 43rd Hawaii International Conference on System Sciences, pp. 1-10 (2010).
16. Yue, C.: Decision theory and methods, Beijing: Science Press (2006).
17. Esmalifalak, M., Shi, G., Han, Z., Song, L.: Bad Data Injection Attack and Defense in Electricity Market Using Game Theory Study. IEEE T Smart Grid **4**, 160-169 (2013) https://doi.org/10.1109/TSG.2012.2224391.
18. Liu, Y., Comaniciu, C., Man, H.: A Bayesian game approach for intrusion detection in wireless ad hoc networks. Proceeding from the 2006 workshop on Game theory for communications and

networks (2006).

19. Sedjelmaci, H., Senouci, S.M., Ansari, N.: Intrusion Detection and Ejection Framework Against Lethal Attacks in UAV-Aided Networks: A Bayesian Game-Theoretic Methodology. IEEE Trans Intell Transp **18**, 1143-1153 (2017) https://doi.org/10.1109/TITS.2016.2600370.
20. Sandberg, H., Amin, S., Johansson, K.H.: Cyberphysical Security in Networked Control Systems: An Introduction to the Issue. IEEE Contr Syst Mag **35**, 20-23 (2015) https://doi.org/10.1109/MCS.2014.2364708.
21. Zhu, J., Zhao, B., Zhu, Z.: Leveraging Game Theory to Achieve Efficient Attack-Aware Service Provisioning in EONs. J Lightwave Technol **35**, 1785-1796 (2017) https://doi.org/10.1109/JLT.2017.2656892.
22. Nguyen, T.H., Wright, M., Wellman, M.P., Singh, S.: Multistage Attack Graph Security Games: Heuristic Strategies, with Empirical Game-Theoretic Analysis. Secur. Commun. Netw. **2018**, 2864873 (2018) https://doi.org/10.1155/2018/2864873.
23. Rass, S., König, S., Schauer, S.: Defending Against Advanced Persistent Threats Using Game-Theory. PloS one **12**, e0168675 (2017) https://doi.org/10.1371/journal.pone.0168675.
24. Jiang, W., Fang, B.-X., Tian, Z.-H., Zhang, H.-L.: Evaluating network security and optimal active defense based on attack-defense game model. Chinese J Comput **32**, 817-827 (2009).
25. Zhang, H.-W., Li, T.: Optimal active defense based on multi-stage attack-defense signaling game. Acta Electonica Sinica **45**, 431 (2017).
26. Liu, L., Huang, C., Fang, Y., Wang, Z.: Network Attack and Defense Game Theory Based on Bayes-Nash Equilibrium. KSII Transactions on Internet and Information Systems (TIIS) **13**, 5260-5275 (2019) https://doi.org/10.3837/tiis.2019.10.024.
27. Lye, K.-w., Wing, J.M.: Game strategies in network security. Int J Inf Secur **4**, 71-86 (2005) https://doi.org/10.1007/s10207-004-0060-x.
28. Benkessirat, S., Boustia, N., Nachida, R.: A New Collaborative Filtering Approach Based on Game Theory for Recommendation Systems. J Web Eng **20**, 303-326 (2021).
29. Xu, X., Wang, G., Hu, J., Lu, Y.: Study on stochastic differential game model in network attack and defense. Secur Commun Netw **2020**, 3417039 (2020).
30. Carin, L., Cybenko, G., Hughes, J.: Cybersecurity Strategies: The QuERIES Methodology. Computer **41**, 20-26 (2008) https://doi.org/10.1109/MC.2008.295.

31. Shapley, L.S.: Equilibrium Points in Games with Vector Payoffs, RAND Corporation, Santa Monica, CA (1956).
32. Wang, Z., Lu, Y., L, X., Li, Z.: Optimal defense strategy selection based on the static Bayesian game. J Xidian Univ **7**, 55-61 (2019).
33. Qian, S., Leiqi, X., Ling, G., Hai, W., Yuxiang, W.: Selection of Network Defense Strategies Based on Stochastic Game and Tabu Search. J Comput Res Dev **57**, 767-777 (2020) https://doi.org/10.7544/issn1000-1239.2020.20190870.
34. Sun, Y., Xiong, W., Yao, Z., Moniz, K., Zahir, A.: Analysis of Network Attack and Defense Strategies Based on Pareto Optimum. Electronics **7**, (2018) https://doi.org/10.3390/electronics7030036.
35. Mishra, B., Smirnova, I.: Optimal configuration of intrusion detection systems. Inf Technol Manag **22**, 231-244 (2021) https://doi.org/10.1007/s10799-020-00319-z.
36. Attiah, A., Chatterjee, M., Zou, C.C.: A Game Theoretic Approach to Model Cyber Attack and Defense Strategies. 2018 IEEE International Conference on Communications (ICC), pp. 1-7 (2018).
37. Osborne, M.J., Rubinstein, A.: Solution Manual for A Course in Game Theory by Martin J. Osborne and Ariel Rubinstein, Boston & London: MIT Press (1994).
38. Wang, Z., Lu, Y., Li, X.: Security Risk Assessment of Military Information Network Based on Attack-Defense Game. Mil Oper Res Syst Eng **33**, 35-40 (2019).
39. Cuong, D., Tran, N., Hong, C.S., Kamhoua, C., Kwiat, K., Blasch, E., Ren, S., Pissinou, N., Iyengar, S.: Game Theory for Cyber Security and Privacy. ACM Comput Surv **50**, 1-37 (2017) https://doi.org/10.1145/3057268.
40. Fudenberg, D., Levine, D.K.: Whither Game Theory? Towards a Theory of Learning in Games. J Econ Perspect **30**, 151-170 (2016) https://doi.org/10.1257/jep.30.4.151.
41. Endsley, M.R.: Situation Awareness Misconceptions and Misunderstandings. J Cogn Eng Decis **9**, 4-32 (2015) https://doi.org/10.1177/1555343415572631.

Figure legends

Fig. 1 The analysis chart of Penetration gains and cost. A graph of the relationship between the benefits of penetration testers and the costs spent is recorded for the three hybrid strategies.

Fig. 2 The analysis chart of defender gains and cost. A graph of the relationship between the benefits of the system defender and the cost spent is recorded for the three hybrid strategies.

Figures

Figure 1

The analysis chart of Penetration gains and cost. A graph of the relationship between the benefits of penetration testers and the costs spent is recorded for the three hybrid strategies.

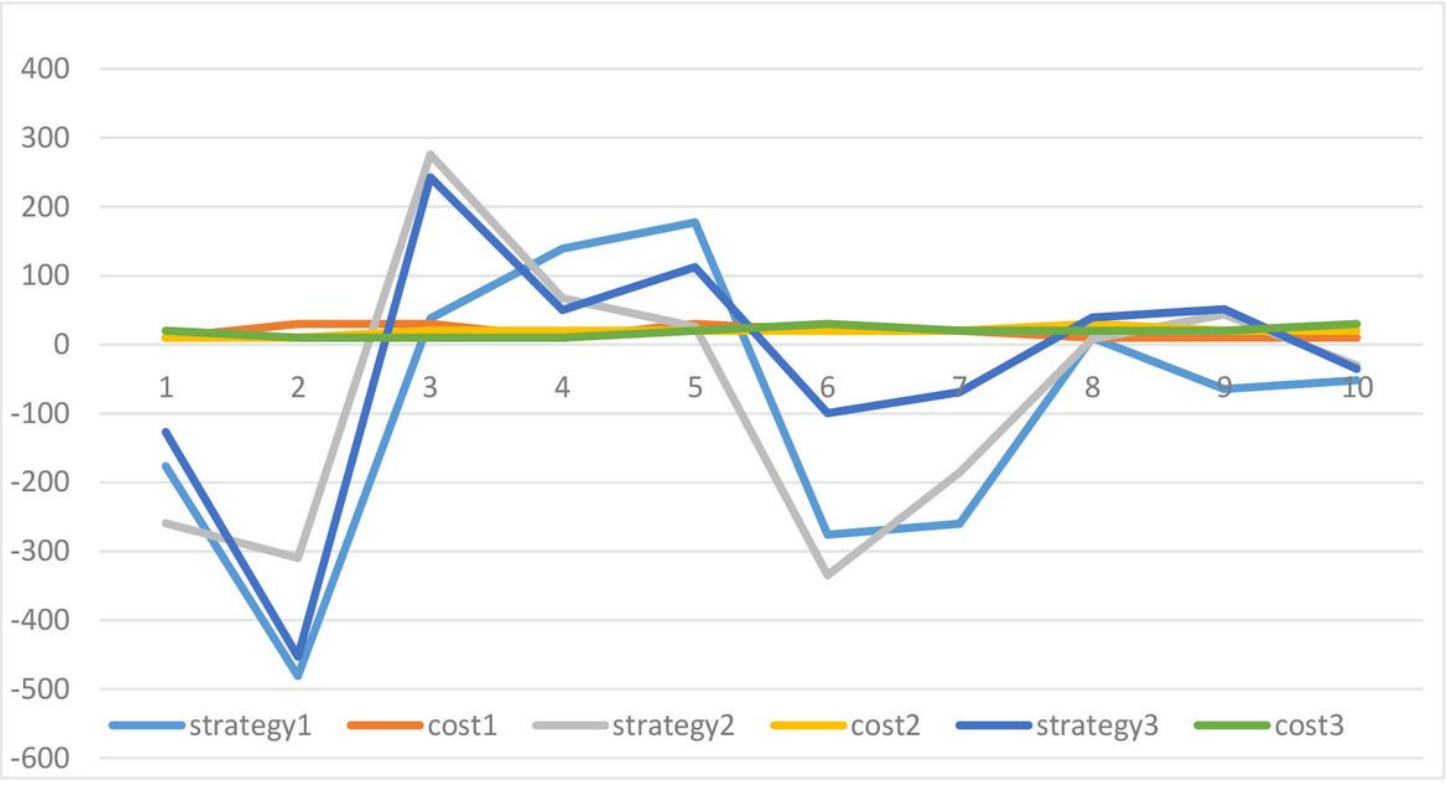

Figure 2

The analysis chart of defender gains and cost. A graph of the relationship between the benefits of the system defender and the cost spent is recorded for the three hybrid strategies.