Effect of Security Investment on Evolutionary Games

CHEN ZHANG[1], RONG PAN[2], ABHIJIT CHAUDHURY[2] AND CHANGXIN XU[3]
[1]*Department of Computer Information Systems*
Bryant University
Smithfield, RI 27519, USA
E-mail: {czhang; achaudhu}@bryant.edu
[2]*China Constructions Bank*
Nanjing, Jiangsu, 2100002, P.R. China
E-mail: panrong2.js@ccb.com
[3]*School of Business*
Hohai University
Nanjing, Jiangsu, 210098, P.R. China
E-mail: xuchxin@hhu.edu.cn

In this paper, we propose an evolutionary game model to analyze the investment decision making process in the cyber offender-defender interaction and provide a quantified approach for defender to calculate the safety threshold to avoid the occurrence of offender-leading game. Then we use simulation as a workbench to discuss the adjustment of each parameter to the security investment threshold. Our evolutionary game model shows that the cyber offender-defender game can possibly reach one realistic stable point after a long-term evolution, which implicates a tied offender-defender game. We found that an offender-leading game can be avoided by maintaining the security investment above a safety threshold level determined by the system vulnerability among other environmental parameters such as residual risk and potential loss. Hence with an optimal level of security investment, the defender can lead the game effectively to discourage attacking attempts. Both linear and nonlinear simulations share similar trends and our evolutionary game theoretic analysis remains valid in either case.

Keywords: management, network reliability, security, artificial intelligence, evolutionary algorithm

1. INTRODUCTION

In recent years, the prevalence, frequency, and severity of cyber-attacks have been growing, as indicated in the annual CSI Computer Crime and Security Survey [38]. The daily number of these attacks increased 93% from 2009 to 2010 [48]. Among Chinese enterprises in traditional industry, as much as 90% have experienced at least one Internet security breach [40]. Major cyber-attacks are also becoming more costly to the victim organizations. A recent survey conducted by McAfee showed that a 24-hour downtime from a major attack was estimated to cost US$6.3 million on average and as much as US$8.4 million a day in the oil/gas sector [3]. The actual frequency of security incidents and the associated financial losses are probably even higher, since organizations may not report all cyber security incidents due to reputational and other concerns, as Gordon, Loeb, and Sohail [19] point out. The increasing frequency and cost of security incidents in recent years highlight the importance of effective cyber security management [18].

Received November 20, 2013; revised February 4, 2014; accepted March 1, 2014.
Communicated by Hahn-Ming Lee.

However, there are multiple challenges to improving cyber security.

First, the information asymmetry unique to this type of attack determines the inferior status of the defenders, who not only cannot forecast the behaviors of the offenders, but also cannot get an accurate understanding of their own defense efficiency or the global level of cyber security. Anderson's [2] research shows that the "Market for Lemons" model put forward by Akerlof [1] is beginning to fit the current market of cyber security products. Vendors all declare that their products can assure security, but the defender cannot determine how these security products differ in quality. The defender, therefore, tends to pay the medium price for a security product instead of choosing a high-quality product with a higher price. Gradually, this may force the high-quality products to withdraw from the market. Even after purchasing and utilizing such security products, many defenders hardly know how to benchmark their own defense efficiency.

Existing research [20] shows that information sharing is beneficial to defenders and can improve the overall social welfare. However, organizations may not report all cyber security incidents due to reputational and other concerns. The lack of reliable information sharing among defenders makes it more difficult for each individual defender to manage the security risks it faces. Moreover, the lack of a motivation mechanism makes defenders tend to adopt the "free-ride" strategy, which leads to further underinvestment in cyber security. Many countries have started to take action to improve this situation, and currently, more than 30 U.S. states have passed laws on revealing security breach information [56]. Li and Rao [30] examine the effects of private intermediaries on optimal timing of disclosure policy made by public intermediaries and vendors' reactions. Their analysis of private intermediaries' role suggests that public intermediary's optimal disclosure time does not change with private intermediary's participation. Besides imperfect mechanism of information disclosure, defenders' enthusiasm to obtain security knowledge is not high. Wang and Xiao [53] investigate the search behavior that drives the search for information security knowledge via a search engine and find that network attacks of current day and one day prior significantly impact the search, while vulnerability disclosure does not significantly affect the search.

Second, return on security investment is difficult to measure, which influences the quality of decision-making. In comparison with financial investments, cyber security investment is characterized as lagged return: that is, the benefit of cyber security investment is not obvious and it sometimes may be perceived as a waste of money when there is no security incident or attacks do not succeed. Cavusoglu and Mishra [7] suggest indirect estimation of the dollar value of losses associated with security breaches as an approximation for the actual cost of security breaches.

Third, while information sharing is challenging for the defenders, it has enabled the rapid development of the offender community. The black-hat community emphasizes knowledge sharing and trading of illegal goods and services, usually through public IRC channels. Franklin [11] reveals the structure of this cyber black market, including the participation, the illegal goods and services, and their pricing. Using a honeypot approach, Holtz [26] found similar structures with more refined role division in the Chinese cyber black market and the geographic distribution of malicious websites.

Fourth, the externality of cyber security further enhances the difficulty of decision-making for the defender. This externality of cyber security, composed of network externalities and externalities of insecurity [34], is manifested in the side effects that each defender imposes on other defenders. Due to network externalities, a defender's decision on network or software platform adoption depends not only on the specific features and functions of the product, but also on the existing scale of adoption. The externalities of insecurity illustrate the fact that a defender with a higher security level increases other defenders' risk of suffering cyber-attacks, since the profit-driven offender generally prefers weaker rivals, given the same conditions. Hence, the externality of cyber security creates an interdependent decision framework for defenders.

Finally, recession-driven cuts in cyber security investment have been very popular recently, according to a survey conducted by McAfee [3]; this further deteriorates the investment environment of the whole society and places defenders in an even more dangerous situation. Practitioners generally regard security investment like any other IT investment and use decision-theoretic risk management to determine their security investment level [28]. Although decision theory and other traditional risk analysis methods can provide a useful starting point for determining security investment level, they are incomplete because of the security problem's strategic nature [6]. Hence, quantification tools considering the strategic nature of the security problem are needed to help determine the appropriate security investment level.

Most organizations have to consider the cost-benefit tradeoff for cyber security investment, and it becomes a critical decision for chief information and security officers. It is not easy for defenders to decide on an appropriate investment level for cyber security. The 2004 Ernst & Young Global Information Security Survey [9] listed budget constraints as one of the main obstacles to effective information security.

These existing challenges for cyber security and the demand among defenders for investment quantification tools prompted us to investigate the criteria for optimal investment level from the perspective of offender-defender interaction. In this paper, we propose a parametric evolutionary game model to analyze the investment decision-making process in the cyber offender-defender interaction and study the impact of cyber security investment level in two-player games. To the defender, the offender-defender recursive interaction is considered to decide the appropriate level of cyber security investment in self-protection. In making this decision, the defender needs to optimize investment in self-protection to manage the risk of a compromise. It is worth notice that since our model is evolutionary, it is different from the models of existing work which is based on the assumption of a single scenario of offender-defender interaction, such as work of Gupta, Chaturvedi, and Mehta [22]. Their model offers the suggestions to investment trade-off between protection and recovery under a specific set of environmental parameters for the scenario.

Our evolutionary game theory (EGT) model shows that the offender-defender game can possibly reach one realistic stable point after recursive interactions, which implicates a tied offender-defender game. We propose a quantified approach for the defender to calculate the safety threshold to avoid an offender-leading game. The higher return on security investment (ROSI) of the safety threshold indicates that the safety threshold is also the optimal investment level. Hence, we believe that with an appropriate level of security investment, the defender can obtain an advantage in the game and effectively discourage attack attempts. Furthermore, we establish both linear and nonlinear simulation instruments as a workbench to discuss the impact of each parameter (residual risk, defense efficiency, and system vulnerability before and after cyber security investment, as well as the comparison between the offender's and the defender's efficiencies) on the security investment threshold.

The contributions of our study are tetramerous. Firstly, we establish a parametric EGT model to analyze the interdependent investment decision-making of cyber offender-defender populations in a recursive interaction. Then we seek the equilibrium state by taking ROI of both players into consideration. This is different from the models in existing works, which is based on the assumption of a single scenario of offender-defender interaction. Our evolutionary game model shows that the cyber offender-defender game can possibly reach one realistic stable state with evolution, which implicates a tied offender-defender game. Secondly, we propose a quantified approach for the defender to determine the appropriate security investment level based on our EGT model. This facilitates understanding of security investment level on the game, enabling defenders to find the security investment threshold avoiding an offender-leading game. We also find that the defender can lead the game effectively to discourage attacking attempts by keeping the investment threshold, which is demonstrated as the optimal investment level by ROSI. These differentiate our research from existing works. We not only establish the investment decision framework and suggest the trend of investment effects for defenders, but also provide the defender a quantified tool to allocate defense resources based upon his/ her own circumstance and need (such as inherent system vulnerability, effectiveness of adopted technologies, acceptable degree of risk tolerance, security management level and attackers faced).Thirdly, we illustrate the impact of each parameter on the security investment threshold by establishing both linear and nonlinear simulation workbenches. The simulation charts offer the defender a visual understanding on the influence of each parameter and facilitate defenders to adjust investment strategies upon their particular needs. Finally, our EGT model is practical. It reflects the best practice since the decision of players in our EGT model represents that of their population. Our EGT model also takes best practice and dynamic decision evolution into consideration by analyzing the decision interaction of two players and their communities in an offender-defender game. Moreover, our EGT model is not limited to a single industry or certain countermeasures. It can be applied to cyber-security budgeting by adjusting the values of parameters.

This paper has a significantly improved model in comparison with our earlier conference paper [37] which has led to the new stable point and more practical applications. This paper discusses the impact of each parameter on the security investment threshold by establishing simulation workbenches and therefore can better support security investment decision making.

We organize this paper as follows: Section 2 reviews the existing work on cyber security investment and introduces the background of theory. Section 3 describes the EGT model to discuss the offender-defender interaction. Section 4 proposes a quantified approach for the defender to calculate the safety threshold to avoid an offender-leading game and illustrates how security investment level impacts the evolutionary outcomes of cyber security two-player games. Section 5 discusses the implications of the research and concludes the paper.

2. RELATED LITERATURE AND BACKGROUND THEORY

Because of the strategic nature of security issues, we believe game theory is more suitable to model the offender-defender interaction. Further, we have adopted EGT because it is better equipped to deal with bounded rationality assumptions and is able to capture the recursive strategic interaction between the offender and the defender. Perfect rationality may not be practical in all cyber-attacks; this is partly due to the asymmetry of game information and partly due to the automation of cyber-attack tools. If one player adopts irrational behavior, classical game theory might fail. Evolving strategies are more practical for cyber security investment decisions because of the internal information asymmetry.

2.1 Related Literature

Security researchers have generally reached a consensus that the existing security problems cannot be solved by technological means alone. Since technological means cannot eliminate all risks, attention is increasingly paid to quantifying the cyber security investment [16, 21, 31, 35, 51], employment of cyber insurance to transfer residual risks [4, 5], the impact of information sharing on cyber security, and how interdependency influences the investment incentive of agents [21, 25, 36].

Studies have been carried out to estimate the information security incident occurrence probability and the incident impact: Kesh [29] developed a framework for analyzing e-commerce security by examining the relationships among e-commerce security needs, threats, technologies, and tools. Geer [15] introduced business adjusted risk (BAR) for classifying security defects by their vulnerability type, degree of risk, and potential business impact. Farahmand [10] presented a subjective analysis, probabilitic assessment, and damage evaluation of information security incidents. Sun [47] developed an evidential reasoning approach under the Dempster-Shafer theory of belief functions for information system risk assessment.

Gordon and Loeb [17] chronicle the development of economics in information security as an academic area of research and they also [21] presented an economic model to determine the optimal information security investment amount. Their research shows that information assets with midrange vulnerabilities are worthier of protection and a firm should invest only a relatively small portion of the expected loss due to a security breach. Wang and Chaudhury [52] introduce the concept of value-at-risk to measure the risk of daily losses an organization faces due to security exploits and use extreme value analysis to quantitatively estimate the value at risk. With this approach, decision makers can make a proper investment choice based on their own risk preference instead of pursuing a solution that minimizes only the expected cost. Hausken [24] analyzed how income, interdependency, and substitution effects impact security investment for organizations of different sizes. Ogut, Menon, and Raghunathan [36] hold the view that interdependency of cyber-risk reduces firms’ incentives to invest in security technologies and to buy insurance coverage. Cavusoglu, Mishra, and Raghunathan [8] proposed a comprehensive analytical model to balance the cost and utility of IT security measures for investment decision support.

Roy, Ellis, and Shiva [41] believe that game theory offers promising perspectives, insights, and models to address cyber security problems. Cavusoglu, Raghunathan, and Yue [6] compared game theory and decision theory methods from several dimensions, including investment levels, vulnerability, and investment payoff, and discussed the limitations of other traditional models.

Longstaff [33] argued that investment in system risk assessment can reduce the likelihood of intrusions, which yields benefits much higher than the investment. Varian [50] examined the free rider problem in information security investment in different circumstances using a game theory model. In their models, both agents, the offender and the defender, maximized their own expected benefits, and it was shown that the reactions of the defender and offender depend on their own cost-benefit ratio. Garcia and Horowitz [14] established a game-theoretic model to analyze the economic motivations for investment in improving cyber security. Their research found that as the ratio of social value to revenue at stake for Internet service providers continues to grow, the likelihood of underinvestment in security becomes higher. Gal-or and Ghose [13] studied economic incentives for sharing security information and found that security investment and security information sharing act as strategic complements in equilibrium. Kannan and Telang [27] considered whether movement toward a market-based mechanism for vulnerability disclosure leads to a better social outcome. Heal and Kunreuther [25] established a parametric game-theoretic model to address the situation in which security choices made by one agent affect the risks faced by others.

Several previous papers have done pioneer work in the context of cyber security by applying EGT. Sun [45, 46] analyzed information security issues based on game theory and EGT respectively and provided strategy suggestions to encourage information security investment. Vejandla [51] investigated an evolutionary approach to generate intruder-defender strategies by introducing a memory-based multi-objective evolutionary algorithm (MOEA) in a simulated network environment. Tembine [49] studied access games, particularly in wireless networks, by applying EGT with a random number of interacting players. Yin and Xia [55] conducted an evolutionary game analysis of the interaction between firewalls and intrusion detection systems and studied factors that play vital roles in the process. These previous works suggest that EGT can provide new insight into cyber security strategies. However, none of the existing work provided a comprehensive discussion of the influence of Replicator Dynamics (RD) and various environmental parameters drawn from the cyber security practice over the ROSI, to the best of our knowledge, leaving a gap which our paper is trying to address.

Offenders, in cyber space, are trying their best to remain anonymous. For example, botnets are often recruited by compromising innocent third parties and launched by peer-to-peer (P2P) communications, making it difficult for defenders and law enforcement to trace them back. However, some potential mitigation techniques, such as content poisoning and Sybil-based and Eclipse-based mitigations, have been proven effective [23]. Therefore, even without considering legal consequences, the offender will still incur costs such as time and effort when s/he performs an attack. Hence, we consider a risk-neutral population of offenders. Defenders, by definition, might need to account for a worst-case scenario. Hence they have to take both proactive and reactive measures to minimize the risk of compromise and the loss from a breach. We consider a risk-neutral population of defenders and give suggestions for risk-averse application of our conclusions later.

2.2 Background of EGT

Game theory is the branch of applied mathematics that formalizes strategic interaction among autonomous rational players, while EGT is the application of game theory to evolution. Classical game theory requires perfect rationality. If the players are not assumed to be rational, EGT applies. Besides the reduced assumption of rationality, another distinction of EGT from traditional game theory is that it allows evolving strategies.

EGT was first put forward by Fisher. In the 1960s, Lewontin began to study ecological matters with EGT. Ecologists Maynard Smith and Price put forward the concept of the evolutionarily stable strategy (ESS) based on a combination of biological evolutionary theory and classical game theory. Generally, the presence of ESS is regarded as the naissance of EGT by academe. Maynard Smith [43] also defines payoff as the game outcome of the players which is a measurement of utility referred by social scientists. Soon, replicator dynamics (RD) was put forward by Taylor and Jonker for the first time. Thereafter, EGT became popular in the fields of sociology and economics. EGT abides by the principle of "survival of the fittest" from biological evolutionary theory and applies it to group behavior. It can interpret the evolutionary process of investors' behavior better than classical theory.

A detailed presentation of EGT can be found in [12, 54]. ESS and RD are two vital concepts in EGT. ESS means a stable state in which a colony or population resists the intrusion of mutation strategy. If this strategy is adopted by all members of a colony and the payoff of this strategy is higher than that of the mutation strategy, the mutation strategy will not intrude upon the colony. Each player who adopts strategy x has a probability $(1 - \varepsilon)$ facing the player who adopts the same strategy x; and probability ε facing the player who adopts the mutation strategy x'. $u(k, s)$ indicates the payoff (utility) of the player adopting strategy k with payoffs. The conditional expression of ESS is as follows:

$$u[x, (1 - \varepsilon) + \varepsilon x'] > u[x, (1 - \varepsilon)x + \varepsilon x'], \tag{1}$$

where ε is an infinitesimal positive number $0 < \varepsilon << 1$.

RD is a dynamic differential equation that describes the proportion of a certain given strategy adopted by a colony. If the payoff (utility) of the given strategy is higher than the average payoff (utility) of the colony, the proportion adopting it in the colony will increase. The differential equation of RD is as follows:

$$dx_k/dt = x_k[u(k, s) - \bar{u}(s, s)], k = 1, \ldots, n, \tag{2}$$

where x_k is the proportion of strategy x adopted by a colony and $\bar{u}(s, s)$ represents the average payoff (utility) of the colony.

3. MODEL

3.1 Hypotheses

We assume there are two types of risk-neutral players with bounded rationality in cyber security investment decisions. One is the population of defenders, who decide whether to invest in improvement of cyber infrastructure for self-protection, and the other is the profit-driven population of offenders, who need to weigh cost against return to decide whether to conduct cyber-attacks. Their decisions are discrete; the defender chooses whether or not to invest in self-defense, and the offender chooses whether or not to perform an attack.

Organizations victimized by a cyber-compromise suffer damages. These damages can be tangible or intangible; they can include financial loss due to fraudulent transactions, interruption of business operations, loss of sensitive data, or loss of reputation and customer confidence, to name a few. We assume the total financial loss is L.

An organization's ability to defend against cyber-attacks depends on its level of self-protection investment, with the assumption that the appropriate defense technology is applied. Ryu and Sharman [42] model a possible deception system with the explicit purpose of enticing unauthorized users and restricting their access to the real system. They found that, under the assumption of a dual entity system, intruders differ in behavior depending on the system's vulnerability at the time of intrusion as well as depending on their own economic incentives. Before the defender makes additional cyber security investment, the probability of a successful attack completely depends on the inherent vulnerability, v_0, of the original system. We define p_0 to be the probability of a compromise before investment in self-protection.

The investment cost of the defender is a one-time infrastructure investment, featuring in its large scale, long period for usage, slow value transfer as well as difficult capital retrieval. After the defender invests I in self-protection of its cyber infrastructure, the offender has a probability p1 of success. Obviously, $p_1 < p_0$. Heal and Kunreuther [25] assume that damages can only occur once, *i.e.*, that damages resulting from multiple security failures are no more severe than damages from a single failure. We assume that the expected financial losses of the defender before and after the cyber security investment are p_0L and p_1L respectively, with the impact of the severity of the vulnerability but without the impact of the frequency of attacks. Obviously, the security investment amount the defender invested I should be less than the economic loss it saved $(p_0-p_1)L$.

E is the normal return from information assets of the defender. The implementation of additional security countermeasures should also increase the cost of attack for offenders. For example, the offender may have to break through more layers of firewalls. The defender invests in self-protection with capital I while the offender incurs a cost of C_1 and C_2 ($C_1 < C_2$) to attack before and after the defender's self-protection investment. Due to the specific features of cybercrime such as anonymity of the criminal, difficulty in tracing back and forensics, the offender in fact only bears extremely low risk of breaching the law compared to her/his high economic profit. Our proposed EGT model, therefore, does not consider offender's cost of breaching the law for the pragmatic goal.

Assuming the offender can derive return R out of a successful attack, then p_1R-C2 represents her/his payoff when the defender invests in self-protection. Likewise, when the defender does not invest in self-protection, the payoff for the offender who performs an attack is p_0R-C1. With the black market of cyber-attacks maturing, the cost of the offender is constantly shrinking, and the high return rate has encouraged the observable rapid growth of a black cyber economy [32, 39].

It is an appointed task for the defender to protect its cyber infrastructure and information assets; therefore, making a cyber security investment cannot bring any immediate profit to the defender (ignore the long-term security reputation gain). Thus, if the defender invests to protect its cyber infrastructure, when the offender succeeds, the defender will face a loss of p_1L. So her/his expected payoff is $E-I-p_1L$. On the contrary, if the defender does not invest in cyber security, s/he can save the additional cyber security investment I, and therefore when suffering attack, her/his payoff is $E-p_0L$.

Obviously, the offender will gain nothing if s/he does not perform an attack. In that case, the payoff for the offender is 0. Likewise, if the offender never attacks, the defender's expected payoff is $E–I$ and E respectively when s/he does and does not invest in self-protection. Detailed list of variable names and meanings is presented in Appendix. Hence, we introduce the payoff matrix of the offender-defender EGT model (in normal form) as:

3.2 RD of the Offender-Defender EGT Model

Assume that in the population of offenders, the proportion that adopts the "Attack" strategy is α. Thus, the proportion that adopts the "Do not attack" strategy is $(1–\alpha)$. Meantime, we denote by parameter β the proportion in the population of defenders that adopts the "Invest" strategy, and by $(1–\beta)$ the proportion that adopts the "Do not invest" strategy.

Table 1. Expected payoff matrix of the evolutionary game between the population of offenders and the population of defenders.

Offender	Defender	
	Invest	Do not invest
Attack	$p_1R–C_2, E–I–p_1L$	$p_0R–C_1, E–p_0L$
Do not attack	$0, E–I$	$0, E$

Hence, the expected utility of the offender population when the "Attack" and the "Do not attack" strategies are adopted, U_{oa}, U_{od}, as well as the average utility of the population, respectively, are

$$U_{oa} = \beta(p_1R–C_2) + (1–\beta)(p_0R–C_1) = –\beta(R(p_0–p_1) + (C_2–C_1)) + (p_0R–C_1) \tag{3}$$
$$U_{oa} = \beta 0 + (1–\beta)0 = 0 \tag{4}$$
$$\bar{U}_o = \alpha U_{oa} + (1–\alpha)U_{od} = \alpha(–\beta(R(p_0–p_1) + (C_2–C_1)) + (p_0R–C_1) \tag{5}$$

The expected utility of the defender populations that adopt the "Invest" and the "Do not invest" strategies are U_{di}, U_{dd} respectively; together with the average utility of the population are

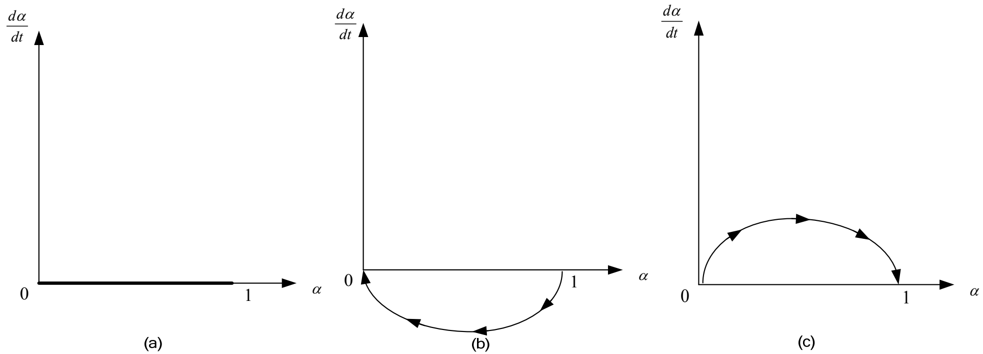
$$U_{di} = \alpha(E–I–p_1L) + (1–\alpha)(E–I) = –\alpha p_1L + E – I \tag{6}$$
$$U_{dd} = \alpha(E–p_0L) + (1–\alpha)E = –\alpha p_0L + E \tag{7}$$
$$\bar{U}_d = \beta U_{di} + (1–\beta)U_{dd} = \beta(\alpha L(p_0 – p_1) – I) – \alpha p_0L + E \tag{8}$$

The RD of this evolution system can be obtained by applying an RD equation to the two populations of players – offender and defender:

$$\begin{cases} \dfrac{d\alpha}{dt} = \alpha(1-\alpha)\big(-\beta\big(R(p_0-p_1)+(C_2-C_1)\big)+(p_0R-C_1)\big) \\ \dfrac{d\beta}{dt} = \beta(1-\beta)\big(\alpha L(p_0-p_1)-I\big) \end{cases} \tag{9a, b}$$

3.3 ESS of the Offender-Defender EGT Model

According to the stability principle of differential equations and the definition of ESS, it is known that when $\beta=(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1))$, $d\alpha/dt$ always equals to 0, *i.e.*, α is in the stable state. When $\beta>(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1))$, $\alpha^*=1$ and $\alpha^*=0$ are two stable states of α. At this time, $\alpha^*=0$ is ESS. When $\beta<(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1))$, $\alpha^*=1$ and $\alpha^*=0$ are still two stable states of α. But $\alpha^*=1$ is ESS at this time. Fig. 1 depicts phase diagrams and stable states when α evolves under the aforementioned three conditions.

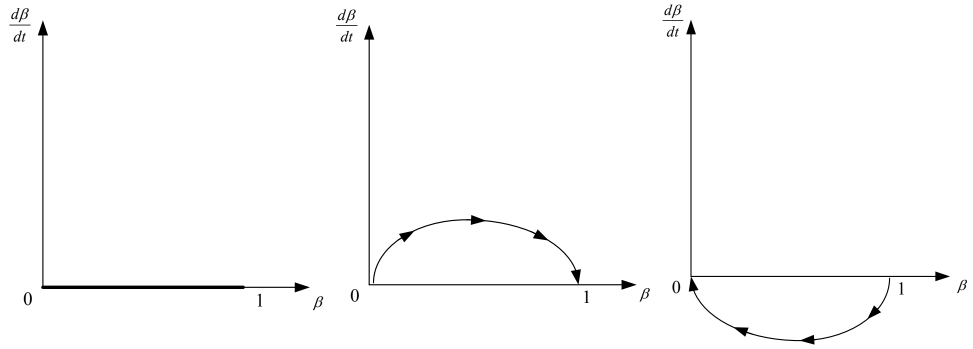


(a) $\beta=(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1))$

(b) $B>(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1))$

(c) $B<(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1))$

Fig. 1. RD phase diagrams of the population of offenders in the asymmetric offender-defender game.



(a) $\alpha=I/(L(p_0-p_1))$

(b) $\alpha>I/(L(p_0-p_1))$

(c) $\alpha<I/(L(p_0-p_1))$

Fig. 2. RD phase diagram of the population of defenders in the asymmetric offender-defender game.

Likewise, when $\alpha=I/(L(p_0-p_1))$, β is in the stable state. When $\alpha > I/(L(p_0-p_1))$, $\beta^*=1$ and $\beta^*=0$ are two stable states of β. At this time, $\beta^*=1$ is ESS. When $\alpha < I/(L(p_0-p_1))$, $\beta^*=1$ and $\beta^*=0$ are two stable states of β, but $\beta^*=0$ is ESS at this time. Fig. 2 provides phase diagrams and stable states when β evolves under the aforementioned three situations.

Detailed stability analysis of the offender-defender EGT model is available upon request.

4. RESULTS AND DISCUSSION

4.1 Effect of the Cyber Security Investment Level

Obviously, only ESS $\alpha^*=1$ and $\beta^*=1$ reflects the real scenario of competing offender-defender game: that is, the population of offenders tends to continue to perform cyber-attacks while the population of defenders tends to persist on investment in cyber security. The two players get even score at the end. In practice, what can we do to impel the drawn game towards a defender-leading one? What is the determinant that helps to avoid the occurrence of dangerous offender-leading game? Let's first examine the problem based on the stability analysis of both sides.

According to the stability analysis for the population of defenders, when the proportion of offenders that adopts the "Attack" strategy α is $I/(L(p_0-p_1))$, the offender-defender interplay ends up with a stable state no matter which strategy the population of defenders chooses. Since the parameter value of α within [0, 1] will possibly cause a tie-game which is undesirable, forcing its value to be 1 or more can effectively avoid the formation of an offender-leading game. Therefore, the benchmark one of defender investment B_1 should be:

$$B_1 = L(p_0 - p_1) + E. \tag{10}$$

In compliance with the aforementioned analysis, when the proportion of the defender population choosing the "Invest" strategy β reaches $(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1))$, the offender-defender interplay ends up with a stable state no matter which strategy the population of offenders chooses. Thus, this equilibrium is the key to achieve the defender-leading game. We denote $\bar{I}=\beta I$ as the average investment level of the entire defender group to facilitate benchmarking with the offender-leading game. Thus,

$$\bar{I}=\beta I=I(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1)). \tag{11}$$

In other words, it is the residual risk that the defender cannot eliminate with a reasonable investment in cyber security. The expression of p_1 can be obtained from (11), which reflects the trend that, given a certain average white hat community investment level, increasing a specific defender's investment will reduce her/his residual risk.

$$p_1 = p_0 + \frac{C_2-C_1}{R} - \frac{I(p_0R-C_1)}{\bar{I}R} \tag{12}$$

In order to discourage attacking attempts of the offender, the defender can take self-protective action by investing in additional cyber security. As discussed earlier, when $\beta>(p_0R-C_1)/(R(p_0-p_1)+(C_2-C_1))$, the expected payoff for the "Attacking" offender is less than the average payoff for the entire offender population. Therefore, the population of offenders will gradually adjust its strategy toward "Do not attack." So, the defender can induce the offender to adopt the "Do not attack" strategy by making an appropriate self-protection investment in cyber security. Because of (11), the defender is expected to reach the following to obtain an advantage in the game. We name it as the benchmark two of cyber security investment B_2:

$$\bar{I} = \beta I = I(p_0R - C_1)/(R(p_0 - p_1) + (C_2 - C_1)). \tag{13}$$

4.2 Discussion of Parameters

Next we propose a quantified approach for defender to calculate the safety threshold to avoid the occurrence of offender-leading game by both linear and nonlinear models based on different expressions of p_0 and p_1 by other environmental parameters. Then we use simulation as a workbench to discuss the impacts of each parameter (residual risk, defense efficiency, system vulnerability before and after the cyber security investment as well as the comparison between the offender's efficiency and the defender's efficiency) to the security investment threshold under the assumption that other parameters will remain constant within a reasonable range. Since our model does not suggest any singular point, we believe the trends of individual parameter from the simulation results reflect their general properties. The two simulations are based in part on the Gordon-Loeb [21] model and the model of Cavusoglu, Raghunathan, and Yue [6], but differ from these works since we analyze the trends of the safety threshold given the increasing probability of a compromise before investment in self-protection.

4.2.1 Discussion of parameters under linear simulation

It is clear that appropriate security investment should be able to deter attacking attempts more effectively. According to (10), the benchmark one for the defender climbs linearly with the increase of p_0. Hence, the raise of p_0 should further discourage the attacking attempts of the offender. We denote the ratio of $d(v_0)=C_2/R=p_0e$ as the discouragement of attack that is impacted by the effectiveness of defense and proportional to p_0, where $(0<e<1)$ and hence is linear. h is used to indicate the comparison between defense efficiency before and after the security investment, $h=(C_2-C_1)/R$. According to the Gordon-Loeb model [21], the optimal investment in information security should be less than or equal to 36.79% of the loss that would be expected in the absence of any investment in security. Hence, the average white hat community investment is $\bar{I}=jL(j<36.79\%)$. Therefore, the benchmark one and two of self-defense investment under the linear simulation B_{1l} and B_{2l} are

$$B_{1l} = L(p_0 - p_1), \tag{14}$$

$$B_{2l} = \frac{\bar{I}\left(R(p_0-p_1)+(C_2-C_1)\right)}{p_0R-C_1} = \frac{\bar{I}\left((p_0-p_1)+(C_2-C_1)/R\right)}{p_0-C_1/R} = jL\frac{p_0-p_1+h}{p_0(1-e)+h}. \tag{15}$$

The two benchmark values intersect at the p_0 value of

$$(1-e)p_0^2 + \left(h-j-p_1(1-e)\right)p_0 - (h-j)p_1 - hj = 0. \tag{16}$$

And the positive solution of this expression of p_0 is:

$$p_0 = \frac{\left(\left(h-j-p_1(1-e)\right)^2 + 4(1-e)\left((h-j)p_1 + h\cdot j\right)\right)^{1/2} - h + j + p_1(1-e)}{2(1-e)}. \tag{17}$$

This is where the two benchmarks intersect in Fig. 3.

ROSI is an important benchmark to decide the optimal security investment level. Practitioners currently apply ROSI as a cyber security investment metric−67.8 percent in 2009, over 44 percent in 2008, trying to find out the appropriate level of investment to prevent recurring security breaches [39]. We calculation ROSI based on Sonnenreich's [44] equation:

$$ROSI = \frac{\left(RiskExposure \bullet \%RiskMitigated\right) - SolutionCost}{SolutionCost}.$$

Under the linear assumptions, we denote ROSI as S_l

$$S_l = \frac{\left(p_0 - p_1\right)L - B_l}{B_l} = \frac{\left(p_0 - p_1\right)L}{B_l} - 1. \tag{18}$$

For our numerical illustration, we use the following parameter values: p_1=0.08, e=0.3, h=0.05, L=R=1 and j=0.25. Since we only discuss appropriate security investment that will reduce security risks, p_0 is more than residual risk p_1. Results are plotted in Fig. 3, which indicates that B_{1l} climbs linearly with the increase of p_0. Meanwhile, with the increase of p_0, B_{2l} becomes stagnant after moderate increase. It is noteworthy that in Fig. 3, the value of B_{1l} is smaller than B_{2l} before their intersection and the trend reverses after the two benchmarks intersect.

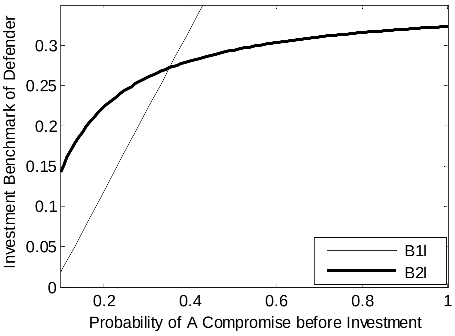


Fig. 3. Benchmark for cyber security investment in linear simulation (p_1=0.08, e= 0.3, h=0.05, L=1, R=1and j=0.25).

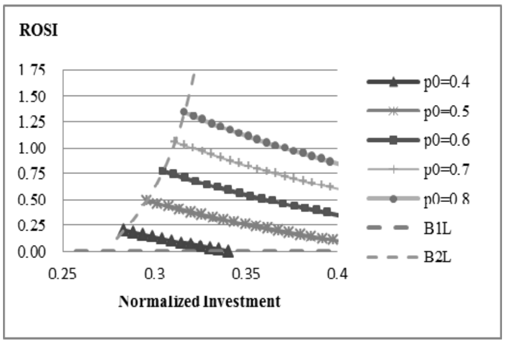


Fig. 4. ROSI in linear simulation (p_1=0.08, e=0.3, h=0.05, L=1, R=1 and j=0.25).

Fig. 4 shows ROSI of B_{1l} and B_{2l} as well as the relationships between ROSI and I with p_0 as parameter respectively under the linear assumptions with the security investment amount varies from the minimum value to maximum value of B_{1l} and B_{2l}. A decreasing trend of ROSI indicates that the minimum value of B_{1l} and B_{2l} is the safety threshold for the defender to achieve the defender-leading game. A higher ROSI of B_{1l} and B_{2l} before and after intersection of the two investment benchmarks indicate that the safety threshold enjoys higher ROSI. The safety threshold, hence, also is the optimal investment level. This is also the optimal security investment normalized by the potential loss.

Fig. 5 plots the safety threshold under linear assumptions. The "Offender-leading Zone" indicates that the defender's self-protection investment is under the safety threshold and the offender-defender game might turn out to be a dangerous offender-leading game. The "Defender-leading Zone" is when the defender's investment has reached the safety threshold and therefore the defender is now leading the game. Hence, with an appropriate level of cyber security investment, the defender can avoid the dangerous offender-leading game and further lead the offender-defender game.

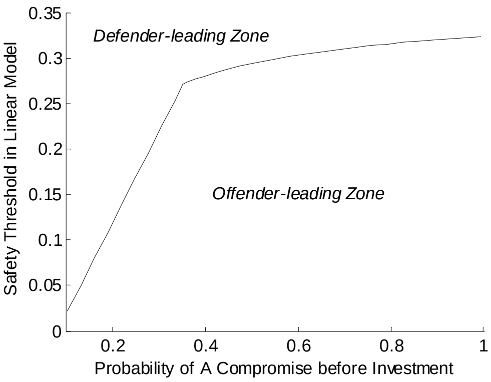


Fig. 5. Safety threshold in linear simulation (e=0.3, h=0.05, L=1, R=1 and j=0.25).

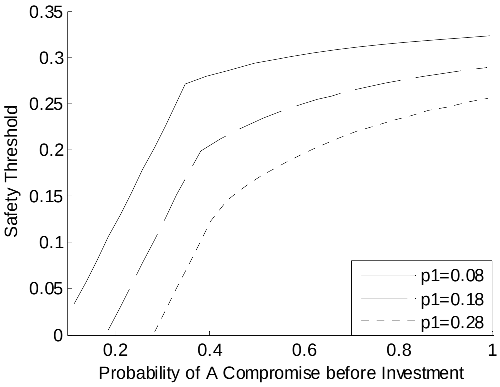


Fig. 6. The impact of residual risk on safety threshold in linear simulation (e=0.3, h=0.05, L=1, R=1and j=0.25).

We then discuss how the residual risk under linear assumptions influences the level of safety threshold. Fig. 6 presents the relationship between p_0 and the safety threshold, with residual risk p_1 varying between 0.08 and 0.28. For our numerical illustration, we use the following parameter values: e=0.3, h=0.05, L=1, R=1 and j=0.25. It can be observed that the residual risk increases with the safety threshold (minimum security investment) decreases. Hence, residual risk is a vital parameter under linear simulation which is controlled by minimum security investment.

4.2.2 Discussion of parameters under nonlinear simulation

Further analysis is conducted under the nonlinear simulation of p_0, p_1 and other environmental parameters. We assume $d(I)=C_2/R=aI^{\sigma}$, where $d(I)$ is the discouragement of attack where ($a > 0$ and $\sigma \geq 0$). The expression of v_0 is assumed based on the assumption that, with the increase of v_0, p_0 will increase at a nonlinear rate (depends on the defense mechanism of a specific system) before becoming stagnant, according to the observation that risk of system compromise will not increase significantly when multiple vulnerabilities lead to similar security consequences. The expression of p_1 is based on the reference of Cavusoglu, Raghunathan, and Yue [6], with the increase of v_0 as well as C_2 and the decrease of I, p_1 will rise at a nonlinear rate before remaining stagnant. Hence

$$p_0 = 1 - bv_0^{-1/\lambda} \tag{19}$$

$$p_1 = kv_0{}^{\varphi} C_2{}^{\theta} I^{-\varpi} = kb^{\lambda\varphi}\left(1-p_0\right)^{-\lambda\varphi} a^{\theta} R^{\theta} I^{\sigma\theta} I^{-\varpi} = a^{\theta} b^{\lambda\varphi} kR^{\theta}\left(1-p_0\right)^{-\lambda\varphi} I^{\sigma\theta-\varpi} \tag{20}$$

where a>0, b>0, k>0, σ≥0, λ≥0, φ≥0, θ≥0, and ω≥0.

Thus, the nonlinear investment benchmark one and two B_{1n}, B_{2n}, ROSI of the defender S_n under nonlinear assumptions, respectively, are as follows:

$$B_{1n} = L\left(p_0 - p_1\right) = L\left(p_0 - a^{\theta} b^{\lambda\varphi} kR^{\theta}\left(1-p_0\right)^{-\lambda\varphi} B_{1n}{}^{\sigma\theta-\varpi}\right) \tag{21}$$

$$B_{2n} = \frac{\overline{I}\left(R\left(p_0-p_1\right)+\left(C_2-C_1\right)\right)}{p_0R-C_1} = \frac{\overline{I}\left(\left(p_0-p_1\right)+\left(C_2-C_1\right)/R\right)}{p_0-C_1/R} \tag{22}$$

$$= jL\frac{p_0-a^{\theta}b^{\lambda\varphi}kR^{\theta}\left(1-p_0\right)^{-\lambda\varphi} B_{2n}{}^{\sigma\theta-\varpi}+h}{p_0-aB_{2n}{}^{\sigma}+h}$$

$$S_n = \frac{\left(p_0-a^{\theta}b^{\lambda\varphi}kR^{\theta}\left(1-p_0\right)^{-\lambda\varphi} B_n{}^{\sigma\theta-\varpi}\right)\left(p_0-aB_n{}^{\sigma}+h\right)}{j\left(p_0-a^{\theta}b^{\lambda\varphi}kR^{\theta}\left(1-p_0\right)^{-\lambda\varphi} B_n{}^{\sigma\theta-\varpi}+h\right)}-1 \tag{23}$$

The explicit expression of the intersection of B_{1n} and B_{2n} is difficult to represent. But our numeric examples show that they have similar attributes as in the linear case, as demonstrated in Fig. 7. For our first numerical illustration, we use the following parameter values: σ=1.5, λ=1, θ=4/3, ω=2/3, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L=1, R=1 and j=0.25. Results are charted in Fig. 7, which indicates that B_{1n} for the defender to lead this cyber security game climbs near-linearly with the increase of p_0. Meanwhile, B_{2n} for cyber security investment becomes stagnant after moderate increase with the growth of p_0. In Fig. 7, similar to the linear model, the value of B_{1n} is smaller than B_{2n} before their intersection and the trend reverses after the two benchmarks intersect.

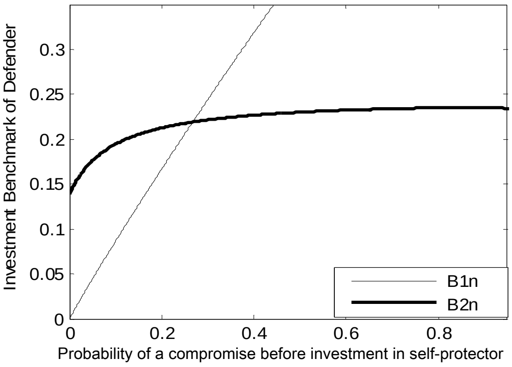


Fig. 7. Benchmark for cyber security investment in nonlinear simulation (σ=1.5, λ=1, θ=4/3, ω= 2/3, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L =1, R=1 and j=0.25).

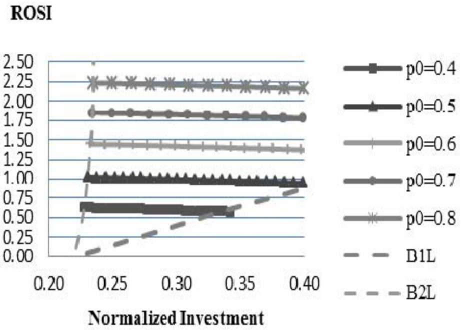


Fig. 8. ROSI in nonlinear simulation (σ=1.5, λ=1, θ=4/3, ω=2/3, φ =0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$ =0.35, h=0.05, L=1, R=1 and j=0.25).

Fig. 8 shows ROSI of B_{1n} and B_{2n} as well as the relationship between ROSI and I with p_0 as a parameter under the nonlinear assumptions with the security investment amount varies from the minimum value to maximum value of B_{1n} and B_{2n}. A consistent decreasing trend of ROSI indicates that the minimum value of B_{1n} and B_{2n} is the safety threshold for the defender to achieve the defender-leading game. A higher ROSI of B_{1n} and B_{2n} before and after intersection of the two investment benchmarks indicate that the safety threshold enjoys higher ROSI. The safety threshold, hence, also is the optimal investment level. Fig. 9 plots the safety threshold under nonlinear assumptions.

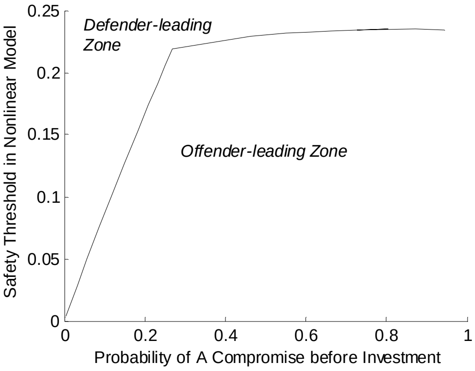


Fig. 9. Safety threshold in nonlinear simulation (σ=1.5, λ=1, θ=4/3, ω=2/3, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L=1, R=1 and j=0.25)

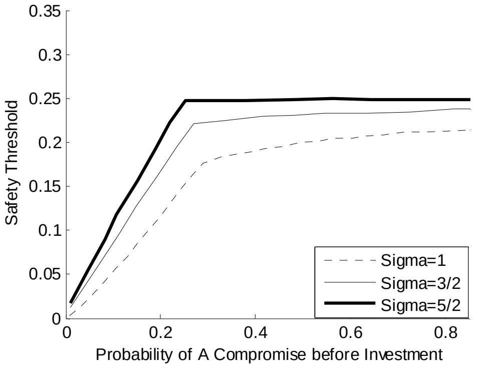


Fig. 10. The impact of sigma on safety threshold in nonlinear simulation (λ=1, θ= 4/3, ω=2/3, φ =0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$= 0.35, h=0.05, L=1, R=1 and j=0.25).

Next, we discuss how each parameter under the nonlinear assumptions affects the security investment level. First, the role of σ is explored with the other parameter values of λ=1, θ=4/3, ω=2/3, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L=1, R=1 and j=0.25. Fig. 10 presents the relationship between p_0 and safety threshold, with σ varying between 1 and 2.5. A larger sigma value indicates a defense technology with lower efficiency; since the defender's normalized investment benchmark value should be less than 1 (hence the security investment is less than the potential financial loss). It is also indicates that, given the same probability of a compromise before investment in self-protection, the higher the defense efficiency (smaller sigma value) is, the lower the safety threshold is.

Second, the influence of λ is analyzed with the other parameter values of σ=1.5, θ= 4/3, ω=2/3, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L=1, R=1 and j=0.25. Fig. 11 presents the relationship between p_0 and safety threshold, with λ varying between 1 and 3 representing the vulnerability of the existing system to the attacks before defense improvement. The larger the value of λ, the less vulnerable the system was to the cyber exploits. Fig. 11 shows that, given the same probability of a compromise before investment in self-protection, the larger λ is, the smaller safety threshold is. This achievement of saving in cyber security investment can be achieved by improving the effectiveness of day-to-day information system security management.

Third, the impact of φ is discussed with the other parameter values of σ=1.5, λ=1, θ=4/3, ω=2/3, a=0.1, $a^{\theta}b^{\lambda\varphi}k$ =0.35, h=0.05，L=1，R=1 and j=0.25. Fig. 12 presents the relationship between p_0 and safety threshold, with φ varying between 0 and 0.25. φ represents the system vulnerability after security investment, which impacts the residual risk.

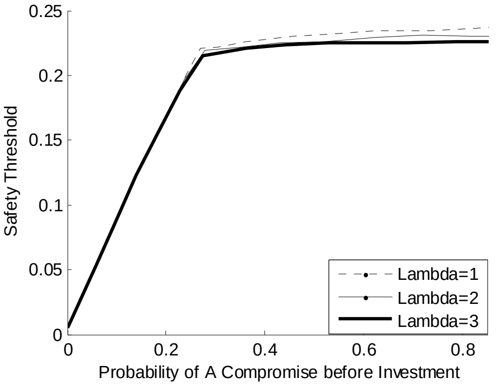


Fig. 11. The impact of lambda on safety threshold in nonlinear simulation (σ=1.5, θ=4/3, ω= 2/3, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L=1, R=1 and j=0.25).

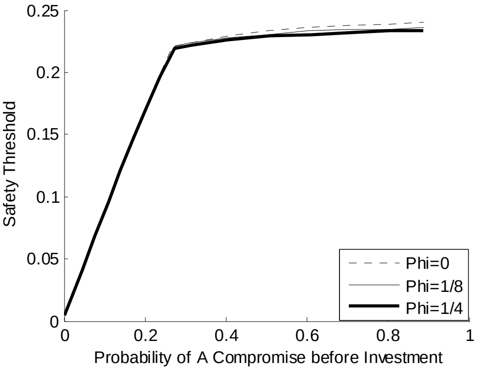


Fig. 12. The impact of phi on safety threshold in nonlinear simulation (σ=1.5, λ=1, θ=4/3, ω=2/3, a=0.1, $a^{\theta}b^{\lambda\varphi}k$ =0.35, h= 0.05, L=1, R=1 and j=0.25).

The larger the value of φ, the higher the residual risk will be. This is because less security investment will result in higher residual risk. The acceptable residual risk level should comply with the information security policy.

The effects of θ and ω are studied by defining μ=$\sigma\theta$−ω, with the other parameter values of σ=1.5, λ=1, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L=1, R=1 and j=0.25. Fig. 13 presents the relationship between p_0 and safety threshold, with μ varying between 1 and 1.5. μ implicates the comparison between the offender's and the defender's efficiency. The larger the μ value, the more efficient the offender is in competition with the defender. According to Fig. 13, given the same probability of a compromise before investment in self-protection, the larger μ is, the larger the safety threshold is.

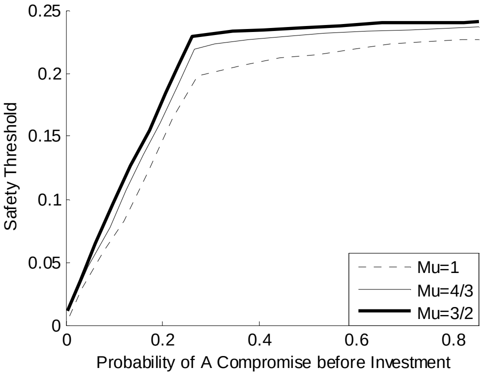


Fig. 13. The impact of mu on safety threshold in nonlinear simulation (σ=1.5, λ=1, φ= 0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L=1, R=1 and j=0.25).

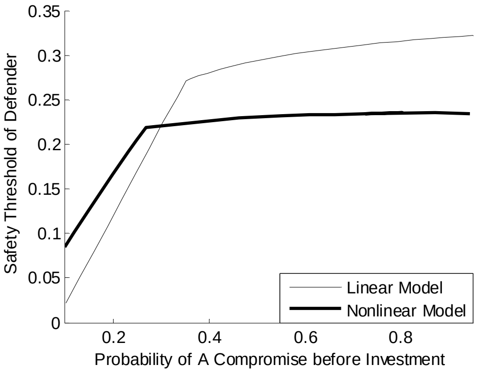


Fig. 14. Benchmark for cyber security investment in linear and nonlinear simulation share similar trends (p_1=0.08, e=0.3, σ=1.5, λ=1, θ= 4/3, ω=2/3, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h= 0.05, L=1, R=1 and j=0.25).

Under the nonlinear simulation, each parameter (defense efficiency, system vulnerability before and after the cyber security investment as well as the comparison between the offender's efficiency and the defender's efficiency) influences the safety threshold level differently. It can be also observed that defense efficiency has the most impact towards the safety threshold while the system vulnerability before investment has the least impact. Besides, the comparison between the offender's efficiency and the defender's efficiency also has a significant influence. This phenomenon is reflected in the attackers' constant upgrade of exploiting tools and the defenders' investment into better countermeasures.

4.2.3 Similarity of linear and nonlinear simulation results

Fig. 14 compares the linear and nonlinear simulations with parameter values of p_1= 0.08, e=0.3, σ=1.5, λ=1, θ=4/3, ω=2/3, φ=0.125, a=0.1, $a^{\theta}b^{\lambda\varphi}k$=0.35, h=0.05, L=1, R=1 and j=0.25. In both simulations, the investment benchmark one for the defender climbs linearly or near-linearly with the increase of probability of a compromise before investment in self-protection. Meanwhile, in both cases, with the increase of probability of a compromise before investment in self-protection, the benchmark two for cyber security investment becomes stagnant after a moderate increase. Overall, the two simulations share similar trends in both investment benchmark values and also in safety threshold.

Hence, the linear or nonlinear assumptions, reflecting the difference in inherent risks to the existing information system and the technological effectiveness of the security remedies, will affect the specific investment benchmark values. But they share similar trends, and our evolutionary game theoretic analysis remains valid in either case.

Quantifying the system vulnerability before and after the application of security investment does pose a challenge for practitioners. However, new automated quantifying tools such as the attack surface metric [58] and model checking [59] can automatically analyze the code of large software systems to provide measures of vulnerability. Additional tools include the historical data analysis tools, AI ranking algorithm tools and fuzzy logic tools as well as tools to analyze the data feedback and perform black box analysis on live information system [57] are constantly providing us with better tools to quantify them. Furthermore, these tools can possibly be combined into some standard model used for industrial benchmarking. Hence we have good reasons to believe that our research will have practical applications in the foreseeable future.

5. CONCLUSION AND FUTURE WORKS

We have proposed an evolutionary game-theoretic model addressing decision making in the cyber security offender-defender interaction from an EGT perspective and providing a quantified approach for the defender to calculate the safety threshold to avoid an offender-leading game. We found that an offender-leading game can be avoided by maintaining the security investment above the safety threshold level determined by the system vulnerability and other environmental parameters such as residual risk and potential loss. With an appropriate level of security investment, the defender can lead the game to effectively discourage attack attempts while still maintaining a reasonable ROSI.

This conclusion can be extended to apply to risk-averse defenders by suggesting an additional investment buffer on top of the threshold to properly adjust to their risk appetite at the price of a reduced ROSI. Next, we designed simulation as a workbench to discuss the adjustment of each parameter to the security investment threshold. Our discussion of both linear and nonlinear simulations explained how each parameter affects the security investment level as well as their similarity in trends.

Our research helps to quantify the appropriate investment level of cyber security. With this quantification approach, an organization can determine proper security solutions based on its cyber security strategy. From the individual organization point of view, a regularly maintained cyber security management system is also more cost-effective than injecting surges of security investment due to the reduction in ROSI. We argue that the prevalence of recession-driven cuts in information security investment [3] is not wise, since they might lead toward an offender-leading game, which might quickly degrade the cyber security environment for e-commerce development. The health of the cyber security ecosystem requires persistent effort from organizations and society.

There are a number of possible directions that can be explored in future studies. Firstly, a multi-agent evolutionary game model including a supervisor, offender, and defender could be established to thoroughly analyze the decision-making process in cyber security investment. With effective global coordinated cyber security governance, attackers' risks and payoffs can be significantly influenced. Secondly, option game theory could be applied to discuss the optimal timing of the proposed safety threshold. Finally, due to the dynamic nature of cyber security, an evaluation and feedback model could be adopted to dynamically fine tune the proposed investment in the long run.

ACKNOWLEDGMENT

We would like to show our deepest gratitude to related reviewers, who have provided us with useful comments on early drafts. All remaining shortcomings are ours.

APPENDIX

Table A1. General expressions in linear simulation.

Variable name	Variable meaning
C_1, C_2 ($C_1 < C_2$)	Attack cost of the offender before and after the defender's self-protection investment
e	A coefficient represents the relationship between discouragement of attack and the probability of a compromise before investment in self-protection
E	Defender's normal return from information assets
h	The comparison between defense efficiency before and after the security investment
I	Investment cost the defender spent in self-protection of its cyber infrastructure
j	The proportion social average investment accounts in the expected loss without cyber security investment
L	Total financial loss of the defender when suffers an successful cyber attack
p_0, p_1 ($p_0 > p_1$)	The probability of a compromise before and after investment in self-protection

R	Return the offender derived out of a successful attack
v_0	Inherent system vulnerability before security investment

Table A2. General expressions in nonlinear simulation.

Variable name	Variable meaning
a	A coefficient representing the relationship between discouragement of attack and investment in self-protection
b	A coefficient representing the relationship between system vulnerability and probability of a compromise before investment in self-protection
k	A coefficient representing the relationship between residual risk and investment in self-protection, system vulnerability and attack cost
σ	An exponent represents the relationship between discouragement of attack and investment in self-protection
λ	An exponent represents the relationship between probability of a compromise before investment in self-protection and system vulnerability
φ	An exponent represents the relationship between probability of a compromise after investment in self-protection and system vulnerability
θ	An exponent represents the relationship between probability of a compromise after investment in self-protection and attack cost of the offender after the defender's self-protection investment
ω	An exponent represents the relationship between probability of a compromise after investment in self-protection and defender's investment
$\mu=\sigma\theta-\omega$	A comparison between the offender's and the defender's efficiency

REFERENCES

1. G. A. Akerlof, "the market for 'lemons': Quality uncertainty and the market mechanism," *The Quarterly Journal of Economics*, Vol. 84, 1970, pp. 488-500.
2. R. Anderson, "Why information security is hard – An economic perspective," in *Proceedings of Annual Computer Security Applications Conference*, 2001, pp. 358-365.
3. S. Baker, S. Waterman, and G. Ivanov, "In the crossfire: Critical infrastructure in the age of cyber war," McAfee, UK, http://newsroom.mcafee.com/, 2009.
4. J. Bolot and M. Lelarge, "Cyber insurance as an incentive for internet security," in *WEIS*, http://weis2008.econinfosec.org/papers/Lelarge.pdf, 2008.
5. R. Böhme and G. Schwartz, "Modeling cyber-insurance: Towards a unifying framework," in *Workshop on the Economics of Information Security*, http://weis2010.econinfosec.org/papers/session5/weis2010_boehme.Pdf, 2010.
6. H. Cavusoglu, S. Raghunathan, and W. T. Yue, "Decision-theoretic and game-theoretic approaches to IT security investment," *Journal of Management Information Systems*, Vol. 25, 2008, pp. 281-304.
7. H. Cavusoglu, B. K. Mishra, and S. Raghunathan, "The effect of internet security breach announcements on market value: Capital market reaction for breached firms and internet security developers," *International Journal of E-Commerce*, Vol. 9, 2004, pp. 69-104.
8. H. Cavusoglu, B. Mishra, S. Raghunathan, "A model for evaluating IT security investments," *Communications of ACM*, Vol. 47, 2004, pp. 87-92.
9. Ernst & Young Global Information Security Survey (GISS), Ernst & Young, USA,

2004, http://www.issa-motorcity.org/files/GlobalInformationSecuritySurvey2004.pdf.

10. F. Farahmand, S.B. Navathe, G. P. Sharp, and P. H. Enslow, "A management perspective on risk of security threats to information systems," *Journal of Information Technology Management*, Vol. 6, 2005, pp. 203-225.
11. J. Franklin, V. Paxon, A. Perrig, and S. Savage, "An inquiry into the nature and causes of the wealth of internet miscreants," in *Proceedings of ACM Conference on Computer and Communications Security*, 2007, pp. 375-388.
12. D. Friedman, "Evolutionary games in economics," *Econometrica*, Vol. 59, 1991, pp. 637-666.
13. E. Gal-or and A. Ghose, "The economic incentives for sharing security information," *Information System Research*, Vol. 16, 2005, pp. 186-208.
14. A. Garcia and B. Horowitz, "The potential for underinvestment in internet security: Implications for regulatory policy," *Journal of Regulatory Economics*, Vol. 31, 2007, pp. 37-55.
15. D. Geer, K. S. Hoo, and A. Jaquith, "Information security: Why the future belongs to the quants," *IEEE Transactions on Security and Privacy*, Vol. 1, 2003, pp. 24-32.
16. L. A. Gordon and M. P. Loeb, "Budgeting process for information security expenditures," *Communications of ACM*, Vol. 49, 2006, pp. 121-125.
17. L. A. Gordon and M. P. Loeb, "Economic aspects of information security: An emerging field of research," *Information System Frontier*, Vol. 8, 2006, pp. 335-337.
18. L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Rochardson, "CSI/FBI computer crime and security survey," Computer Security Institute, USA, http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf, 2005.
19. L. A. Gordon, M. P. Loeb, and T. Sohail, "A framework for using cyber insurance for cyber-risk management," *Communications of ACM*, Vol. 46, 2003, pp. 81-85.
20. L. A. Gordon, M. P. Loeb, and W. Lucyshyn, "Information security expenditures and real options: A wait-and-see approach," *Computer Security Journal*, Vol. 19, 2003, pp. 1-7.
21. L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information System Security*, Vol. 5, 2002, pp. 438-457.
22. M. Gupta, A. Chaturvedi, and S. Mehta, "Economic analysis of tradeoffs between security and disaster recovery," *Communications of Accounting Information Systems*, Vol. 28, 2011.
23. D. T. Ha, G. Yan, S. Eidenbenz, and H. Q. Ngo, "On the effectiveness of structural detection and defense against P2P-based botnets," in *Proceedings of Dependable Systems and Networks*, 2009, pp. 297-306.
24. K. Hausken, Income, "Interdependence and substitution effects affecting incentives for cyber investment," *Journal of Accounting and Public Policy*, Vol. 25, 2006, pp. 629-665.
25. G. Heal and H. Kunreuther, "Interdependent security: The case of identical agents," *Journal of Risk and Uncertainty*, Vol. 26, 2002, pp. 231-249.
26. J. Zhuge, T. Holtz, C. Song, J. Guo, X. Han, and W. Zuo, "Studying malicious websites and the underground economy on the Chinese Web," *Managing Information Risk and the Economics of Security*, 2009, pp. 225-244.
27. K. Kannan and R. Telang, "Market for software vulnerabilities? Think again," *Management Science*, Vol. 51, 2005, pp. 726-740.

28. E. Karofsky, "Return on security investment: Calculating the security investment equation," *Secure Business Quarterly*, Vol. 1, 2001.
29. S. Kesh, S. Ramanujan, and S. Nerur, "A framework for analyzing e-commerce security," *Information Management and Computer Security*, Vol. 10, 2002, pp. 149-158.
30. P. Li and H. R. Rao, "An examination of private intermediaries' roles in software vulnerabilities disclosure," *Information System Frontier*, Vol. 9, 2007, pp. 531-539.
31. W. Liu, H. Tanaka, and K. Matsuura, "Empirical-analysis methodology for information-security investment and its application to reliable survey of Japanese firms," *Information and Media Technology*, Vol. 3, 2008, pp. 464-478.
32. M. E. Locasto, A. Stavrou, and A. D. Keromytis, "Dark application communities," in *Proceedings of New Security Paradigms*, 2006, pp. 11-18.
33. T. A. Longstaff, C. Chittister, R. Pethia, and Y. Y. Haimes, "Are we forgetting the risks of information technology?" *Computer*, Vol. 33, 2000, pp. 43-51.
34. T. Moore and R. Anderson, "Economics and internet security: A survey of recent analytical, empirical and behavioral research," Computer Science Group, Harvard University, USA, ftp://ftp.deas.harvard.edu/techreports/tr-03-11.pdf, 2011.
35. M. Negrete-Pincetic, F. Yoshida, and G. Gross, "Towards quantifying the impacts of cyber attacks," in *PowerTech*, http://energy.ece.illinois.edu/gross/papers/powertech-2009final.pdf, 2009.
36. H. Ogut, N. Menon, and S. Raghunathan, "Cyber insurance and IT security investment: Impact of independent risk," in *WEIS*, http://infosecon.net/workshop/pdf/56.pdf, 2005.
37. R. Pan and C. Xu, "Research on decision of cyber security investment based on evolutionary game model," *Multimedia Information Networking and Security*, 2010, pp. 491-495.
38. J. Penn and H. Shey, "Forrsights: The evolution of IT security," 2010-2011, Forrester, USA, http://www.forrester.com/rb/Research/forrsights_evolution_of_it_security%2C_2010_to/q/id/56886/t/2, 2011.
39. S. Peters, "CSI computer crime & security survey," Computer Security Institute, USA, http://www.personal.utulsa.edu/~james-childress/cs5493/CSISurvey/CSISurvey2009.pdf, 2009.
40. Security report of Chinese enterprises, Rising, China, http://www.rising.com.cn/about/news/rising/2011-03-11/9056.html, 2010.
41. S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *Proceedings of Hawaii International Conference on System Sciences*, 2010, pp. 1-10.
42. C. Ryu, R. Sharman, H. R. Rao, and S. Upadhyaya, "Security protection design for deception and real system regimes: A model and analysis," *European Journal Operational Research*, Vol. 201, 2010, pp. 545-556.
43. J. M. Smith, "Game theory and the evolution of behavior," *Behavior and Brain Science*, Vol. 7, 1984, pp. 95-101.
44. W. Sonnenreich, "Return on security investment (ROSI) – A practical quantitative model," *Journal of Research and Practice in Information Technology*, Vol. 38, 2006, pp. 45-56.
45. W. Sun, X. Kong, D. He, and X. You, "Information security investment game with penalty parameter," in *Proceedings of International Conference on Innovative Com-*

puting Information and Control, 2008, pp. 559.
46. W. Sun, X. Kong, D. He, and X. You, "Information security problem research based on game theory," in *Proceedings of Symposium on Electronic Commerce and Security*, 2008, pp. 554-557.
47. L. Sun, R. P. Srivastava, and T. J. Mock, "An information systems security risk assessment model under Dempster-Shafer theory of belief functions," *Journal of Management Information Systems*, Vol. 22, 2006, pp. 109-142.
48. Internet security threat report, Symantec, USA, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_2011_21239364.en-us.pdf, 2011.
49. H. Tembine, E. Altman, R. El-Azouzi, and Y. Hayel, "Evolutionary games with random number of interacting players applied to access control," in *Proceedings of International Conference on Modeling and Optimization in Mobile*, *Ad Hoc*, *and Wireless Networks*, 2008, pp. 344-351.
50. H. R. Varian, "System reliability and free riding," in *Economics of Information Security*, Kluwer Academic Publishers, MA, 2004, pp. 1-15.
51. P. Vejandla, D. Dasgupta, A. Kaushal, and F. Nino, "Evolving gaming strategies for attacker-defender in a simulated network environment," in *Proceedings of IEEE Social Computing*, 2010, pp. 889 -896.
52. J. Wang, A. Chaudhury, and H. R. Rao, "A value-at-risk approach to information security investment," *Information System Research*, Vol. 19, 2008, pp. 106-120.
53. J. Wang, N. Xiao, and H. R. Rao, "Drivers of information security search behavior: An investigation of network attacks and vulnerability disclosures," *ACM Transactions on Management Information Systems*, Vol. 1, 2010.
54. J. W. Weibull, *Evolutionary Game Theory*, MIT Press, Cambridge, MA, 1997.
55. Y. Yin and Z. Xia, "An evolutionary game analysis of the interaction with firewall and intrusion detection system," in *Proceedings of the 8th International Conference on Machine Learning and Cybernetics*, 2009, pp. 2787-2791.
56. L. Zhang, W. J. Hao, and J. Wu, "Introduction about disclosure system of security breach information in U.S.," in *Proceedings of WNCS*, 2010, Vol. 25.
57. W. Jansen and P. D. Gallagher, "Directions in security metrics research," NIST Computer Security Report, http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf, 2009
58. P. K. Manadhata and J. M. Wing, "An attack surface metric," *IEEE Transactions on Software Engineering*, Vol. 37, 2011, pp. 371, 386.
59. B. Schwarz, H. Chen, D. Wagner, J. Lin, W. Tu, G. Morrison, and J. West, "Model checking an entire Linux distribution for security violations," in *Proceedings of the 21st Annual Computer Security Applications Conference*, 2005, pp. 13-22.

Chen Zhang (张晨) is an Associate Professor of Computer Information Systems at Bryant University. His research generated over twenty publications. Chen holds a Ph.D. degree in Computer Science from the University of Alabama and a B.S. in Physics from Tsinghua University. His research interests include management of computer networks, knowledge and technological innovation, data analysis and data mining.

Rong Pan (潘蓉) received the B.S. degree in Computer Science and Technology, the M.S. degree in Economics of Population, Resource and Environment, and the Ph.D. degree in Management Science and Engineering from Hohai University, Nanjing, China. Her research interests include investment management of cyber security, sustainable development of commercial bank and regional industry development.

Abhijit Chaudhury is a Professor of Information Systems at Bryant University. He earned a bachelor's degree in Mechanical Engineering and master's degree in Operations Research from IIT Kharagpur, India. He holds a Ph.D. in Management Information Systems from Purdue University. He is co-author and co-editor of several books on Information Systems.

Changxin Xu (许长新) received the B.S. degree in Mathematics Department of Southeast University, Nanjing, China, received the M.S. degree in Institute of Quantitative Eonomics from Shanghai University of Finance Economics, Shanghai, China, and the Ph.D. degree in College of Harbor Coastal and Offshore Engineering from Hohai University, Nanjing, China. He has been a Professor as well as doctoral supervisor with the Business School, Hohai University, and been the head of Investment Institute of Hohai University.