3-1-2010

Modelging IT Security Investment in Target Group of Similar Firms: A Control Theoretic Approach

Deng Pan Liu
dengpan.liu@uah.edu

Tridib Bandyopadhyay

Modeling IT Security Investment in Target Group of Similar Firms: a Control Theoretic Approach

Deng Pan Liu
University of Alabama, Huntsville
dengpan.liu@uah.edu

Tridib Bandyopadhyay
Kennesaw State University
tbandyop@kennesaw.edu

ABSTRACT

Criminal-hacker nexus leads to a 2 step target selection process, which begins with a short list of firms with similar information assets from which the hacker finally picks up that firm which has the weakest defense. This translates into a scenario where firms with similar information assets engage in a veiled race so as not to appear as the soft target in the focus group. In this work we propose a duopolistic model and utilize a differential game framework to analyze the IT security investment decisions of two firms who find themselves in such a short list of hacking targets and must compete dynamically on their IT security investments to reduce the risk of being breached. We provide the steady state (singular region) analysis of the differential game for two firms with symmetric and asymmetric parameters. Our model exhibits that hacker learning and firms' security investment efficiency have opposite effects on the two equilibrium outcomes of interest, namely, the security level and the security investment rate. As hacker learning improves (security investment efficiency increases), the security levels and security investment rate of the two firms move apart (closer).

Keywords

IT Security, IT Security Investment, Control Theoretic Approach, Optimal Control in IT Security

1. INTRODUCTION

Profitable association with criminals has quite transformed hacker motivation to attack unauthorized computers. Motivations like gaining swaggering rights, exhibiting technical skills and enjoying playful thrills have given way to purely criminal, gain-seeking behavior as dictated by the criminals, who now engage hackers for stealing information assets of value. Also, severe commoditization of Credit and Debit Card numbers, in terms of open availability and high volume of supply in the black market, have driven prices so low that cyber criminals have now been compelled to revise their game plans. Single sign-on login credentials for organizations (e.g. Citrix log-in access based on SSO) and FTP accounts now-a-days fetch premium prices; healthcare related information as well as email exchanges are now traded for high gains[1]. Another popular hacking target in the face of the current downturn in the global economy is intellectual property; stealing proprietary marketable information assets is cheaper than creating them through painstaking initiatives in innovation[2].

We pose this interesting question at this point: '*Given that hackers now work for the criminals, how does this nuance the security landscape in which a firm must defend its IT assets?*' Unfortunately, there is no straightforward answer to this question, and there are no obvious insights available from the extant research in IT security. In order to explain such nuanced IT defense, we argue that the intent and the modus operandi of hacking activities need to be explained from 2 angles: first from the perspective of the principals of the hacking attacks, namely the criminals, and then from that of their agents, i.e., the hackers. Consider a criminal intending to steal the Citrix SSO log-in access of a medical practice into a large healthcare provider network/repository:

(a) The malevolent intent of a criminal in cyber crime stems from his/her downstream contacts and accomplices to utilize the derived information to buy/sell illegal drugs or set up fake web-based drug stores. (Similarly, a stolen SSO access to the Outlook express of an equity research analyst is a prized possession to criminals having skills in pump and dump schemes, because they can now utilize the Outlook access to analyze the exchanges of the official e-mails of that stock analyst.) As a result, the malevolent intent of the criminals, in view of their strengths in downstream activities, segregates defending firms into ***disparate target groups*** of firms who possess similar information assets. The development of such target groups of firms is also supported by a large section of the IT security practitioners in the US: about a fifth of those respondents who suffered one or more kinds of security incidents confirmed that they had suffered a targeted attack aimed exclusively at their organization, or *organizations within a small subset of the general population* (CSI survey 2007). In mid-July 2007, The

[1] Malicious page of The Month, (May 2008). Fijian Malicious Code Research Center,(http://www.finjan.com/Content.aspx?id=1367)
[2] Ackerman et. al. (2009). Unsecured Economies, Protecting Vital Information. McAfee Report.

Washington Post reported attacks on the computers belonging to the U.S. federal government, contractors and companies in the ***transportation industry***. A report from Message Labs also suggests that narrowly targeted attacks are becoming more popular (www.DarkReading.com April 18, 2007).

(b) Criminals employ hackers to gain the access to the information asset. For our examples in point-1 above, the skills that the criminal would look for in a hacker are in terms of penetrating fortified network perimeters and hijacking ports, including gaining FTP accesses. However, hackers tend to compromise/access the specified information asset by spending the lowest amount of effort in order to maximize his/her return. This incentivizes a hacker to ***further select a soft target*** in the first set of target victims which was separated by the criminal's intent (point-1 above). Hackers achieve this intermediate goal by scoping their potential victims' defense systems through footprinting, fingerprinting, information enumeration and dry runs.

In view of (1) and (2) above, certain considerations tend to emerge for the defender of a cyber attack. ***First,*** a firm needs to assess its information assets in terms of their unauthorized sale/use, and then ascertain the group of firms from where a potential hacker could access such similar assets. For example, an inherent security issue for both Facebook and MySpace is the presence of third-party applications (http://www.eweek.com, Dec17, 2008). ***Second***, having identified the target group that it belongs to, a firm needs to competitively invest in IT security such that it can offer relatively higher resistance to a hacker than a comparable firm, in order not to appear as the soft target in the group of similar firms. In other words, a firm needs to harden its IT security only enough to deter and divert a potential abuser, who would then gravitate to a softer target that may require relatively less effort to compromise. That relative strength in defense can divert hackers to the less prepared/secured firm is evidenced in reality. In a sample of 18 financial firms, a 2004 study by the Financial Services Authority (FSA) of UK found that hackers routinely preferred smaller financial firms who also exhibited lower levels of security investments/preparedness.

Finally, as a result of the above shift in attack dynamics, firms with similar information assets (from the criminal's perspective) are now likely to find themselves as *competing targets* for hackers. In this work, we analyze the investment strategies of such similar firms in their endeavor not to appear as the soft target of a hence identified target group. In particular, here we propose a duopolistic model of competing IT security investment between *two* firms in the same target group. Our adoption of a stylized duopoly model brings out managerial insights that are important, relevant and timely, but keeps our analytics tractable. We choose a control theoretic approach for our analysis because of our intention to analyze the relative investments of the firms on a continuous time profile.

The contribution of this work is two-fold. We provide a model for the nuanced IT security defense in view of the established fact that hacking activities are quite criminalized today. This helps us analyze the implicit competition among similar firms' IT security investments facing a scheming hacker. Secondly, we analyze such competition in IT defense within a framework of differential game, and utilize control theoretic approach in the continuous time. To the best of our knowledge, none of this has been done before. Significantly, our work brings out the facts that hacker learning and IT investment efficiency play major roles in the way they determine the level of comparative investment in firms' IT security investment: we exhibit a dilution effect on the investment of the firms as investment efficiency increases as well as a spreading out effect on firms' investment as hacker learning increases because of the experiential gains of the hacker from the scoping and hacking activities.

In what follows, we briefly review the relevant literature in Section 2, present the notation and the analysis of our model in Section 3, and provide our concluding remarks in Section 4. This is a research in progress where we plan to analyze a central planners' solution and compare the investment levels of the firms between the regimes of parochial and coordinated IT security investment.

2. LITERATURE REVIEW

Our current work relates to the interdependence of IT security investment among target firms, and here we provide a brief review of the closely related literature. Research in the economics of information systems literature address investments in IT security. Gordon and Loeb (2002) analyze how security vulnerabilities moderate firms' IT security investments, which Tanaka et. al. (2005) empirically corroborates. Varian (2002) identifies existence of free riding behavior in firms where he views IT security in the light of public good being provisioned by private entities. Kunreuther and Heal (2003) analyze this interdependence of firms' IT security, and characterize the free riding behavior. Hausken (2006) analyzes IT security investment as impacted by firms' interdependence, income, and substitution effects; and later (Hausken (2007)), substitutability and complementarities of IT security investments. Ogut et al. (2005) differentiate security investments between technological controls and cyber insurance instruments and show general complementarity between these instruments. Bohme et. al. (2006) show that correlated cyber risks may create deficiencies in the supply of suitable cyberinsurance instruments, while Bandyopadhyay et. al. (2009) argue that IT managers face implicit losses leading to perceived contract overpricing in the demand side of cyberinsurance products. Sharing of Information about IT security/breaches have also been studied to analyze interdependent IT security investments: Gordon, Loeb, and Lucyshyn

(2003) show that sharing security information reduce firm's incentives to invest in IT security, while Gal-Or and Ghose (2005) argue that IT security investments and information sharing could also feature as strategic complements. The study of differential games was initiated by Isaacs (1965) with applications to warfare and pursuit-evasion problems. A control theoretic approach to solve differential games has been utilized in several works (Sethi et. al 2000), Dockner et. al (2000) yet remained limited to advertising and military games to investigate simultaneous Nash equilibria, and later to investigate Stackelberg equilibria in Supply Chain scenarios.

3. THE MODEL AND ANALYSIS

The differential game in our model is set up in the backdrop of duopolistic competition between Firms A and B in their bid not to appear as the preferred target for an attacking hacker. Each of these firms possesses similar information assets which is the subject of interest to a criminal. In order to compromise the information asset, the criminal engages a hacker, who in turn attempts to optimize her own efforts during the process of compromising the above information asset. In the following paragraphs we first present our assumptions and notation, before we present the objective function that the players attempt to minimize. Next, we present the Hamiltonians, propose the non-singular solutions, and discuss their analytical tractability for singular solutions. Finally we present the singular solutions of our model first under further assumption of symmetry between the firms (analytical), and then we relax this specific assumption of symmetry and present a numerical analysis.

3.1 Assumptions and Model

Firstly, we assume that firms *A* and *B* are substitutable to each other from the hackers' point of view, and that the hacker has the capability to assess the vulnerability level of the firms utilizing standard scoping activities, including those of foot and finger printing tactics over the Internet. In other words, after scoping activities, the hacker can compare the relative vulnerability levels of the firms, and channel more hacking attempts toward the softer target. We present below the notation used in our model and analysis.

x_A (x_B):	The vulnerability level of firm *A* (*B*). This is defined as the probability of breach given an attack by the hacker. ***State Variables***
$N(t)$	The aggregate attacking traffic at time *t*
L_A (L_B)	Loss suffered firm by firm *A* (*B*) from a realized breach
$S_A(t)$ ($S_B(t)$)	The rate of IT security investment by firm *A* (*B*). ***Control Variables***
$S_{\max}$	The maximum rate of IT security investment by either firm *A* (*B*)
$\lambda_A(\lambda_B)$	The current value adjoint (shadow) variable
r	The discount rate, assumed same for either firm *A* (*B*)
β_A (β_B)	The investment efficiency parameter of firm *A* (*B*)
ρ	The time rate of increase in vulnerability of a firm as a reflection of the Hackers' learning effect, assumed same for either firm *A* (*B*)

Table 1: Notation Used in Our Analysis

Secondly, we assume that the proportion of hacking attempts targeted at firm A and B at any instant as $(h(t) = (1 + x_A - x_B)/2)$ *and* $(1 - h(t) = (1 + x_B - x_A)/2)$ which preserves the aggregate hacking rate and the relative impact of the vulnerability levels of the firms. A firm's security level depends on the security investment of that firm, vulnerability levels $x_A(t)$ and $x_B(t)$ are functions of $S_A(t)$ and $S_B(t)$. Consequently, the state equations are[3]:

$$\dot{x}_A = -\beta_A S_A(t) x_A + \rho, \quad x_A(0) = a \qquad \textbf{(1)}$$

$$\dot{x}_B = -\beta_B S_B(t) x_B + \rho, \quad x_B(0) = b \qquad \textbf{(2)}$$

Thirdly, we assume that firm *A* (*B*)'s losses due to penetration/breach is an increasing function of the amount of attacking attempts on the firm *A* (*B*). *Lastly*, the discount rate *r* captures the current value of summated investments for a firm in our infinite-horizon model. Firm A's objective is to minimize the losses from breach through IT security investment, and thus Firm A solves (Firm B solves the analog problem): $Min\{\int_0^\infty ((1/2)N(t)(1+x_A-x_B)x_A L_A + S_A(t))e^{-rt}dt\}$ where $x_A L_A$ is the

[3] *a* and *b* are the initial vulnerability level of firms A and B respectively.

expected loss of firm A from one attacking attempt, and $N(t)(1+x_B - x_A)/2$ is the amount of attacking traffic at firm A. Firms A and B's objective functions can be rewritten as

$$Max\{\int_0^\infty (-(1/2)N(t)(1+x_A - x_B)x_A L_A - S_A(t))e^{-rt}dt\} \quad \textbf{(3)}$$

$$Max\{\int_0^\infty (-(1/2)N(t)(1+x_B - x_A)x_B L_B - S_B(t))e^{-rt}dt\} \quad \textbf{(4)}$$

3.2 General Analysis

Firstly, the current-value Hamiltonians for these firms, based on the state equations (1) and (2), and the objective functions (3) and (4), can be written as

$$H_A = -(1/2)(1+x_A - x_B)x_A L_A + \lambda_A \rho - (1+\beta_A \lambda_A x_A)S_A \quad \textbf{(5)}$$

$$H_B = -(1/2)(1+x_B - x_A)x_B L_B + \lambda_B \rho - (1+\beta_B \lambda_B x_B)S_B \quad \textbf{(6)}$$

Where λ_A and λ_B are the current-value adjoint variables for firms A and B respectively.

From (5) and (6), the Hamiltonians are linear in the control variables (S_A and S_B), and we have the following bang-bang[4] and singular solution form for S_A and S_B.

S_A: 0 if $-(1+\beta_A\lambda_A x_A) < 0$ **To *be Determined*** if $-(1+\beta_A\lambda_A x_A) = 0$ S_{max} if $-(1+\beta_A\lambda_A x_A) > 0$	S_B: 0 if $-(1+\beta_B\lambda_B x_B) < 0$ ***To be Determined*** if $-(1+\beta_B\lambda_B x_B) = 0$ S_{max} if $-(1+\beta_B\lambda_B x_B) > 0$

The controls in the singular region are required to satisfy the following conditions (7).

$$(H_i)_{S_i} = 0, \quad \text{and} \quad (\dot{H}_i)_{S_i} = d(H_i)_{S_i}/dt = 0, \quad i = A, B \quad \textbf{(7)}$$

As for the current-value adjoint variables λ_A and λ_B, we also have the following equations.

$$d\lambda_A/dt = r\lambda_A - \partial H_A/\partial x_A = r\lambda_A - (-x_A L_A + x_B L_A/2 - \beta_A \lambda_A S_A) \quad \textbf{(8)}$$

$$d\lambda_B/dt = r\lambda_B - \partial H_B/\partial x_B = r\lambda_B - (-x_B L_B + x_A L_B/2 - \beta_B \lambda_B S_B) \quad \textbf{(9)}$$

Solving equations (7) - (9) and (1) - (2), we have

$$-r + \beta_A L_A x_A^2 - \beta_A L_A x_A x_B/2 - \rho/x_A = 0 \quad \textbf{(10)}$$

$$-r + \beta_B L_B x_B^2 - \beta_B L_B x_A x_B/2 - \rho/x_B = 0 \quad \textbf{(11)}$$

where $\hat{x}_A$ and $\hat{x}_B$, the singular levels of firms' vulnerability, are the solutions of the above two equations. Since (10) and (11) do not yield closed form solutions, we separately discuss the symmetric and unsymmetrical cases below.

3.3 Symmetric Firms

The symmetric case assumes equality between corresponding parameters of the two firms. When $L_A = L_B = L$ and $\beta_A = \beta_B = \beta$, we have $\hat{x}_A = \hat{x}_B = \hat{x}$, which is a solution of $\beta L x^2/2 = r + \rho/x$. From (1) and (2), both $\hat{x}_A$ and $\hat{x}_B$ are positive constants, thus in the singular period, $\hat{S}_A = \hat{S}_B = \hat{S} = \rho/(\beta\hat{x})$, i.e., *both firms make identical and constant rate of security investment in the singular region*. In the pre-singular region, for firm A, if (i) $a > \hat{x}_A$, (i.e., the initial vulnerability level is higher than that in the singular level), then $S_A = S_{\max}$, (ii) if $a < \hat{x}_A$, then $S_A = 0$; and (iii) if $a = \hat{x}_A$, then $S_A = \hat{S}_A$. The pre-singular region solutions for firm B can be derived in a similar fashion. Also, in the symmetric case, $d\hat{x}/dL < 0$, $d\hat{x}/d\beta < 0$, $d\hat{x}/d\rho > 0$, $d\hat{S}/dL > 0$, $d\hat{S}/d\rho > 0$, and $d\hat{S}/d\beta < 0$. Below we summarize the above results.

[4] Discreet controls at either Maximum controlling force or Complete absence of any controlling force, no intermediate levels are optimal.

Proposition 1:

If the two firms are symmetric, then they both make the same constant rate of security investment in the singular region.

Proposition 2:

The vulnerability level of each firm increases if 1) the Loss from a Breach decreases, 2) the security investment efficiency decreases, or 3) the hackers' learning effect increases.

The singular level of security investment rate of each firm increases if 1) the Loss from a Breach increases, 2) the security investment efficiency decreases, or 3) the hackers' learning effect increases.

3.4 Asymmetric Firms

In the asymmetric case, we conduct numerical analysis due to the difficulty of obtaining analytical results. The baseline values of the model parameters as assumed are $\beta_A = 1$, $\beta_B = 2$, $L_A = 100$, $L_B = 300$, $\rho = 0.6$, and $r = 0.1$.

3.2.1 Impact of Security Investment Efficiency on Security: In this subsection, we choose the baseline values for all the parameters except for β. Here we take $\beta_A = \beta_B = \beta$, and vary the value of β from 0.1 to 10. Consistent with our results for the symmetric case, each firm's vulnerability level goes down as security investment efficiency improves (Figure 1). Firm B, which has a higher loss of a breach (i.e., $L_B > L_A$), has a lower vulnerability level in the singular region.

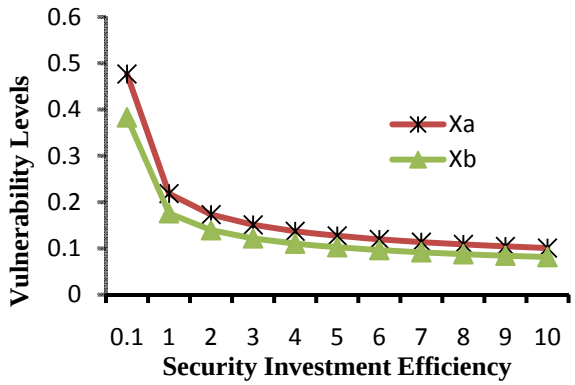

Figure 1: The Impact of Investment Efficiency (β) on the Vulnerability Levels of Firms

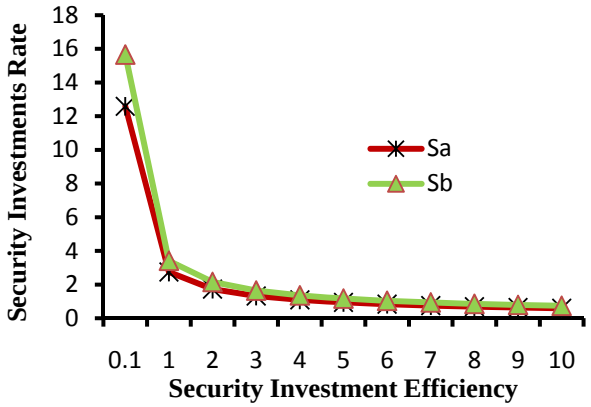

Figure 2: The Impact of Investment Efficiency(β) on the Security Investment Rates of Firms

The difference between the vulnerabilities of the two firms (i.e., $\hat{x}_A - \hat{x}_B$) goes down as well, as the security investment efficiency improves. This indicates that an improvement in the security investment efficiency may ***dilute*** the difference of firms' vulnerability in the singular region, suggesting a relatively more balanced attacking traffic, since the amount of attacking traffic is a function of the difference of the two firms' vulnerability levels. Similarly, the improvement of the security investment efficiency also dilutes the difference of firms' security investment rates in the singular region (Figure 2).

3.2.2 Impact of Hackers' Learning Effect on Security: In this subsection, we choose the baseline values for all the model parameters except for ρ, which we vary from 0.1 to 1.

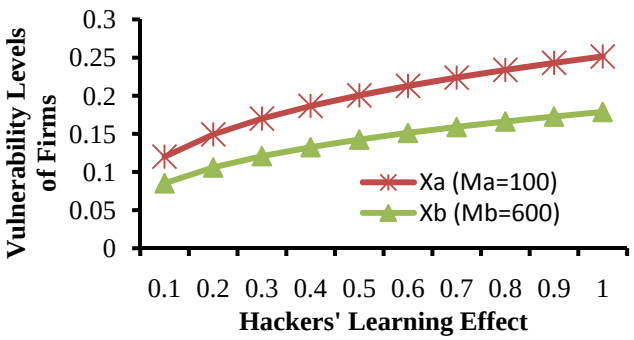

Figure 3: The Impact of Hackers' Learning Effect (ρ) on the Vulnerability Levels of Firms

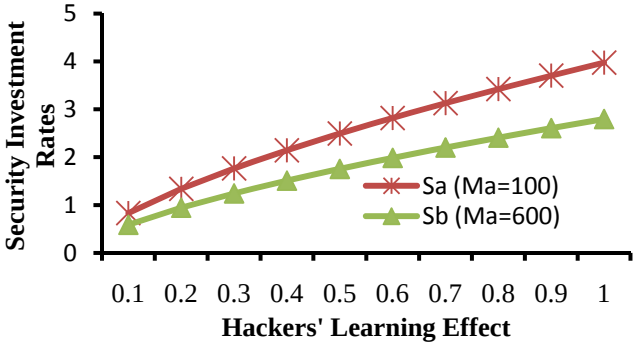

Figure 4: The Impact of Hackers' Learning Effect(ρ) on the Security Investment Rates of Firms

We conveniently substitute $M_i = \beta_i L_i$, and define M_i to be the Efficiency-Loss parameter for firm i, $i = \{A, B\}$. Note that both firms' vulnerability levels increase as hacker's learning effect increases (Figure 3), which is again consistent with our findings in the symmetric case. Note that the firm with the lower value of Efficiency-Loss parameter is more insecure. Interestingly, the gap between the vulnerability levels of these two firms increases with Hackers' leaning. This happens because the firm with higher value of Efficiency-Loss parameter tends to secure its systems more effectively, and thus is less sensitive to hackers' learning effect. This 'spreading-out' effect in the gap of firms' vulnerability levels result in a higher proportion of attacking traffic target the firm with a lower Efficiency-Loss. We also observe a similar 'spreading-out' effect in Figure 4, where the gap between the security investment rates of these two firms increases as hackers' learning effect increases. Also note that, the firm with lower Efficiency-Loss parameter has a higher security investment rate (Figure 4), a result that reflects that the security investment efficiency chosen for that firm is relatively lower.

4. CONCLUDING REMARKS:

We have employed a differential game approach to examine how two firms on a substitutable short list of hacking targets compete dynamically on IT security investments to reduce the risk of being breached. We have shown analytically how the firms' security levels and investment rates change with model parameters in the case where two firms are symmetric. In the asymmetric case, we have shown that hacker learning and the security investment efficiency have a spreading-out effect and a diluting effect, respectively, on the security levels and security investment rates of the two firms. The analysis of our model provides guideline for managers to strategically plan their security investment rates at a particular time and estimate their security levels effectively in a relative sense that occurs in a dynamic, competitive environment of the modern business. There are several interesting issues that are worth studying in the future research. For instance, we propose to study the optimal security investment paths from a central planer's perspective, compare IT security investments under individual and coordinated decision regimes and also identify an effective coordination scheme for the two firms when the social solution offers more beneficial levels of IT security defense for the firms under consideration.

References

1. Bandyopadhyay, T., Mookerjee, V. S., Rao, R. C. 2009. Why IT managers don't go for cyber-insurance products. Communications of the ACM. 52(11). 68-73.
2. Bohme, R., Kataria, G. 2006. Models and Measures for Correlation in Cyber Insurance. In the Proceedings of the Workshop on the Economics of Information Security. Boston, USA.
3. Dockner, E., S. Jorgensen, N.V. Long, G. Sorger. (2000). Differential Games in Economics and Management Science. Cambridge University Press, Cambridge, UK.
4. Gal-Or, E., and Ghose, A. (2005). The Economic Incentive of Sharing Information. Information Systems Research. 16(2), 186-208.
5. Gordon L. A., and Loeb M. P. (2002). The Economics of Information Security Investment. *ACM Transactions on Information and System Security*. Vol. 5, No. 4, 438-457.
6. Gordon, L. A., Loeb, P. M., and Lucyshyn W. 2003. Sharing Information on Computer System Security. Journal of Accounting and Public Policy. Vol. 22.
7. Hausken, K. (2006). Income, Interdependence, and Substitution Effects Affecting Incentives for Security Investment. *Journal of Accounting and Public Policy* 25, 6, 629-665.
8. Isaacs, R. (1965). Differential Games. Wiley, New York
9. Kunreuther, H., Heal, G., 2003. Interdependent security. *The Journal of Risk and Uncertainty* 26, 2/3, 231-249.
10. Ogut H., Raghunathan, S., and Menon N. 2005. Cyber Insurance and IT Security Investment: Impact of Interdependent Risk. In the proceedings of The Workshop on The Economics of Information Security. Cambridge, MA. June 2-3.
11. Sethi, S. and Thompson, G. L. (2000). Optimal Control Theory: Applications to Management Science and Economics. Kluwer Academic Publishers. Boston, USA.
12. Tanaka H,, Matsuura K., and Sudoh O. (2005). Vulnerability and Information Security Investment: an Empirical Analysis of E-local Government in Japan. *Journal of Accounting and Public Policy*. Vol. 24, No. 1, 37-59.
13. Targeted hacking attacks tipped to rise. December 20, 2005. Can be accessed at http://news.zdnet.co.uk/security/0,1000000189,39242899,00.htm
14. Varian Hal. (2002). System Reliability and Free Riding. Working Paper. The University of California at Berkeley.