Dynamics for Proactive Defense through Self-hardening in the Presence or Absence of Anti Malicious Software

Hemraj Saini
Assistant Professor, Department of IT, Orissa Engineering College, Bhubaneswar

T. C. Panda
Professor and Principal, Orissa Engineering College, Bhubaneswar

Bimal Kumar Mishra
Reader, Department of Applied Mathematics, Birla Institute of Technology, MESRA, Ranchi

Minaketan Panda
PG Student, Department of Computer Science, IIIT, Bhubaneswar

ABSTRACT
In computer networks, the computers can be categorized into two categories, one is susceptible or healthy and another is infected. The susceptible computers can have the Anti Malicious Software (AMS) or can not have to protect themselves from the malicious objects. In addition they can have a costly action to self-harden themselves against the malicious objects for proactive defense. The utility cost of being susceptible or infected is the major concern of this paper. The paper considers the role of AMS and the self-hardening action to find out the lifetime utility of a computer. This lifetime utility is beneficial to take the decision, whether the self-hardening/AMS has to be implemented in the computer network or not as it is costly action to protect the computer network from malicious objects.

Categories and Subject Descriptors
K.6.5 [**Security and Protection**]: *Invasive software*---I.6.5 [**Model Development**]: *Modeling Methodologies*

General Terms
Security, Theory, Design

Keywords
Malicious Objects, Anti Malicious Objects, System Hardening, Computer Utility, Prevalence

1. INTRODUCTION
Modeling of malicious objects is one of the most suitable ways to understand their propagation in the network. Many of the models [1, 2, 3, 4, 5] are available in the literature in this direction. The available models are mostly concentrated only for understanding the propagation but very few models [6, 7] concentrated to find out the utility of a computer in the continuum of computers. Utility of a computer in the whole network is one of the important factor to decide whether the imposed security measures [8, 9] such as running an Anti Malicious Software (AMS) [3, 4, 5] or providing system hardening [10] are optimal to proactively defend [8] the computer in network or not.

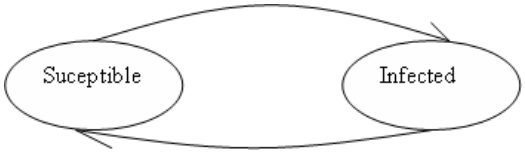

Figure 1: SI model

Our work is giving a direction towards the utility factor of a computer in two cases. First, is in the presence of AMS and self-hardening capability of computer and second, in the absence of AMS and self-hardening capability of computer. Optimality principle [11] is used to calculate the lifetime utility of a computer. Here, we assumed that the computer in a network remains live for a finite time but it will be in either of a state from susceptible/healthy or infected as shown if figure 1. In either of a case it has to pay some cost in the form of protecting itself or recovering from the infected state. The lifetime utility is to be found for an infinite time but it can be easily calculated for a finite time also by our modeled equations. Finally the paper deals to find the different proportions of the utility to predict their dynamics.

The whole paper is divided into following sections-

Section-II: Nomenclature and formulation of the model

Section-III: Discussion of the results

Section-IV: Conclusion and future direction

2. MODEL DEVELOPMENT
2.1 Nomenclature
u_1 = Utility of being infected

u_2 = Utility of being susceptible or healthy

c_1 = Utility cost for self-hardening

c_2 = Utility cost of securing a healthy or susceptible computer

c_3 = Utility cost of being healthy or susceptible

β = Probability of infecting of a susceptible computer which is having no AMS and not to self-harden

β_v = Probability of infecting of a susceptible computer which is having AMS and to self-harden

δ = Probability of death (resources can not be recovered) of an infected computer in a time of span

x = A variable belongs to set R_+

y = A variable belongs to set R_+

$F_t(x, y)$ = A function gives the proportion of computers in period t with AMS and self-hardening

f = density function of $F_t(x, y)$

P_t = Probability of contacting an infected computer who is infected in any period t

$V_v(P_t)$ = Value of a susceptible computer with AMS and having probability P_t of contacting an infected computer in any period t

$V_n(P_t)$ = Value of a susceptible computer without AMS and having probability P_t of contacting an infected computer in any period t

$Q_v(P_t)$ = Lifetime value of a susceptible computer with AMS and having probability P_t of contacting an infected computer in any period t

$Q_n(P_t)$ = Lifetime value of a susceptible computer without AMS and having probability P_t of contacting an infected computer in any period t

2.2 Model Formulation

Consider a population consisting of a continuum of computers, each of whom can be either susceptible or otherwise infected with an infectious malicious object. Assume that, once infection occurs, computers do not remain infected for the remainder of their lives. They can be again converted in to the susceptible computers due to the anti-malicious software. The utility of being infected is u_1, and the utility of being susceptible and healthy is u_2, where, $u_2 > u_1 \geq 0$. Let the utility at death of the computer (resources can not be recovered) be 0. Time is discrete, and, in any period, a susceptible computer has the option of taking a costly action to self-hardening against the risk of infection. Assume that the self- hardening action is perfectly effective at blocking transmission of the infection. The utility cost of self-hardening is $c_1 > 0$, so that if a susceptible computer chooses to self-update in some period, then the computer's net utility in that period is $u_2 - c_1$.

Suppose that anti-malicious software for the infection exists and that every susceptible computer can also choose to be secured in any period at a utility cost of $c_2 > 0$. Assume that, in any period, the decision to be secured precedes the decision of whether or not to adopt the self-hardening action. Implementing anti-malicious software reduces a susceptible computer's chances of acquiring the infection from contacts with infected computers. While susceptible computers having no anti-malicious software that chooses not to self-update becomes infected with probability $\beta \in (0,1]$ after one contact with an infected computer, the corresponding probability for a susceptible computer after implementing anti-malicious software is $\beta_v \in [0, \beta)$. Thus, the anti-malicious software decreases the transmission probability of the infection, and the efficacy of the anti-malicious software can be measured by $(\beta - \beta_v)/\beta \in (0,1]$. If $\beta_v > 0$ then the anti-malicious software does not confer sterilizing immunity. Assuming that, the anti-malicious software offers lifelong immunity. Given any $x \in R_+$ and $y \in R_+$, let $F_t(x, y)$ denote the proportion of computers in period t with anti-malicious software implementation cost $c_2 \leq x$ and self-hardening cost $c_1 \leq y$. Hereafter, a computer with anti-malicious software cost c_2 and self-hardening cost c_1 will be referred to as a $type-(c_2, c_1)$ computer. For simplicity, it is assumed that a computer's expected life span is independent of infection status. Let a computer died (resources can not be recovered) at the end of the period with probability $\delta \in (0,1)$, which is also the mortality rate given a continuum of computers. Note that the expected lifetime utility of an infected computer is therefore u_1/δ. Assumed that, the population size is constant over time and $F_t(x, y) = F(x, y)$ for all *t, x,* and *y*. Assume that the joint distribution function *F* is continuous, and denote its density function by *f*.

All computers can communicate to each other, without considering their status, infected or not, in every period. A susceptible computer can come in the contact of the infected computer, which is characterized by proportional mixing, so that the probability of contacting an infected computer who is infected in any period *t* is given by the proportion of computers who are infected in that period *Pt* . Taking current and the future prevalence of the infection as given, the decision problem of a susceptible computer in each period is to maximize expected lifetime utility by choosing whether or not to take the self-hardening action and, if anti-malicious software has not implemented at the computer, whether to do so or not. Given the stated assumptions of the model, consider the following two cases for the optimization problem of a susceptible computer.

***Case 1*: Susceptible computer with anti-malicious software.**

Using dynamic programming [12], the optimization problem of a susceptible computer with anti-malicious software in period *t* is given by the optimality equation

$$V_v(P_t) = \max\left\{u_2 - c_1 + (1-\delta)V_v(P_{t+1}), u_2 + (1-\delta)[\beta_v P_t \frac{u_1}{\delta} + (1-\beta_v P_t)V_v(P_{t+1})]\right\} \quad (1)$$

Where, $V_v(P_t)$ is the value of the computer in period *t.* The first expression in the maximand is the value of self-hardening in period *t,* and the second expression gives the value of risky behavior in that period.

***Case 2*: A susceptible computer with no anti-malicious software**.

Letting $V_n(P_t)$ denote the value of a computer without anti-malicious software in period *t*, $V_n(P_t)$ solves the optimality equation

$$V_n(P_t) = \max\left\{V_v(P_t) - c_2, u_2 - c_1 + (1-\delta)V_n(P_{t+1}), u_2 + (1-\delta)[\beta P_t \frac{u_1}{\delta} + (1-\beta P_t)V_n(P_{t+1})]\right\}. \quad (2)$$

The first expression in the maximand, $V_v(P_t) - c_2$, gives the value of being a computer with anti-malicious software in period *t* at cost c_2. The second expression is the value of self-hardening in period *t* without getting anti-malicious software, while the last expression is the computer's value with no self-hardening or vaccination in period *t*.

Letting
$Q_v(P) \equiv V_v(P) - u_1/\delta$, $Q_n(P) \equiv V_n(P) - u_1/\delta$, and $w \equiv u_2 - u_1$, equations (1) and (2), respectively, can be rewritten as

$$Q_v(P_t) = \max\{w - c_1 + (1-\delta)Q_v(P_{t+1}), w + (1-\delta)(1-\beta_v P_t)Q_v(P_{t+1})\} \quad (3)$$

and

$$Q_n(P_t) = \max\{Q_v(P_t) - c_2, w - c_1 + (1-\delta)Q_n(P_{t+1}), w + (1-\delta)(1-\beta P_t)Q_n(P_{t+1})\} \quad (4)$$

Using the solutions to the optimization problems in (3) and (4), the notations employed in the derivations are introduced below.

- $A_{v,t}(c_2,c_1)$: The proportion of type-(c_2,c_1) susceptible computers without AMS in period *t* who choose to self-harden in that period.
- $A_{n,t}(c_2,c_1)$: The proportion of type-(c_2,c_1) susceptible computers without AMS in period *t* who choose to not self-harden in that period.
- $B_{v,t}(c_2,c_1)$: The proportion of type-(c_2,c_1) susceptible computers without AMS in period *t* who choose to be with AMS but not self-harden in that period.
- $B_{n,t}(c_2,c_1)$: The proportion of type-(c_2,c_1) susceptible computers without AMS in period *t* who choose not to self-harden and not to be with AMS in that period.
- $C_t(c_2,c_1)$: The proportion of type-(c_2,c_1) susceptible computers with AMS in period *t* who choose not to self-harden in that period.
- $S_t(c_2,c_1)$: The proportion of type-(c_2,c_1) computers who are without AMS and susceptible in period *t*.
- $I_t(c_2,c_1)$: The proportion of type-(c_2,c_1) computers who are infected in period *t*.
- $V_t(c_2,c_1)$: The proportion of type-(c_2,c_1) computers who are with AMS and susceptible in period *t*.

Note that

$$A_{v,t}(c_2,c_1) + A_{n,t}(c_2,c_1) + B_{v,t}(c_2,c_1) + B_{n,t}(c_2,c_1) = 1$$

and $S_t(c_2,c_1) + I_t(c_2,c_1) + V_t(c_2,c_1) = 1$

for all t, c_v and c_s.

With the stated model assumptions, the proportion of type-(c_v,c_s) susceptible computers without AMS in period *t* who survive to period *t* +1 as infected computers are $(1-\delta)P_t[\beta_v B_{v,t}(c_2,c_1) + \beta B_{n,t}(c_2,c_1)]$. Analogously, $1-\delta$ is the proportion of type-(c_2,c_1) susceptible computers with AMS in period *t* who remain alive in period *t* + 1, and, of those, the fraction $P_t\beta_v C_t(c_2,c_1)$ is infected. Therefore, the infection prevalence among type-(c_v,c_s) computers evolves over time according to the following system of equations:

$$S_{t+1}(c_2,c_1) = (1-\delta)[A_{n,t}(c_2,c_1) + B_{n,t}(c_2,c_1)(1-\beta P_t)]S_t(c_2,c_1) + \delta, \quad (5)$$

$$I_{t+1}(c_2,c_1) = (1-\delta)[I_t(c_2,c_1) + [S_t(c_2,c_1)(\beta_v B_{v,t}(c_2,c_1) + \beta B_{n,t}(c_2,c_1)) + V_t(c_2,c_1)\beta_v C_t(c_2,c_1)]P_t], \quad (6)$$

$$V_{t+1}(c_2,c_1) = (1-\delta)[V_t(c_2,c_1)(1-\beta_v C_t(c_2,c_1)P_t) + S_t(c_2,c_1) \times (\sigma_{v,t}(c_2,c_1) + B_{v,t}(c_2,c_1)(1-\beta_v P_t))]. \quad (7)$$

In the steady state for all t the above equations can be re-written as follows-

$$S(c_2,c_1) = (1-\delta)[A_n(c_2,c_1) + B_n(c_2,c_1)(1-\beta P)]S(c_2,c_1) + \delta, \quad (8)$$

$$I(c_2,c_1) = (1-\delta)[I(c_2,c_1) + [S((c_2,c_1)(\beta_v B_v(c_2,c_1) + \beta B_n(c_2,c_1)) + V(c_2,c_1)\beta_v C(c_2,c_1)]P], \quad (9)$$

$$V(c_2,c_1) = (1-\delta)[V(c_2,c_1)(1-\beta_v C(c_2,c_1)P) + S(c_2,c_1) \times (A_v(c_2,c_1) + B_v(c_2,c_1)(1-\beta_v P))]. \quad (10)$$

Hence the lifetime utility for above mentioned both the cases can be given by following equations-

$$Q_v(P) = \max\{w - c_1 + (1-\delta)Q_v(P), w + (1-\delta)(1-\beta_v P)Q_v(P)\} \quad (11)$$

$$Q_n(P) = \max\{Q_v(P) - c_2, w - c_1 + (1-\delta)Q_n(P), w + (1-\delta)(1-\beta P)Q_n(P)\} \quad (12)$$

Here P is an aggregation of the density function $f(c_2,c_1)$.

Note that, since $Q_n(P) \geq (w-c_1)/\delta$ for all P, $Q_n(P) > (w-c_1)/\delta - c_2$ for all P. Therefore, in a steady state, no susceptible computer would choose to adopt the self-hardening action after being with AMS, i.e. $A_v(c_2,c_1) = 0$ for all c_2 and c_1.

Consequently, Eq. (12) reduces to

$$Q_n(P) = \max\left\{\frac{w}{\delta + (1-\delta)\beta_v P} - c_2, \frac{w-c_1}{\delta}, \frac{w}{\delta + (1-\delta)\beta P}\right\} \quad (13)$$

Given P, define the functions $\gamma_n(P)$ and $\gamma_v(P)$, respectively, as follows:

$$\frac{w-\gamma_n(P)}{\delta}=\frac{w}{\delta+(1-\delta)\beta P} \qquad (14)$$
$$\frac{w-\gamma_v(P)}{\delta}=\frac{w}{\delta+(1-\delta)\beta_v P}$$

It is easy to see that both $\gamma_n(P)$ γ and $\gamma_v(P)$ are increasing in P. The benefit to a susceptible computer of having AMS without self-hardening given steady state prevalence P is

$$B(P)=\frac{w}{\delta+(1-\delta)\beta_v P}-\frac{w}{\delta+(1-\delta)\beta P}$$

Using Eqs. (11) and (13), the optimal behavior for type-c_v, c_s susceptible computers in a steady state given prevalence P can be characterized as follows, assuming that, in the case of indifference, computers choose the action that carries the lowest risk of infection:

$$C(c_2,c_1)=\begin{cases}1; if\ldots c_1>\gamma_v(P)\\ 0; otherwise,\end{cases}$$
$$A_n(c_2,c_1)=\begin{cases}1; if\ldots c_1\le\gamma_n(P) and\ldots c_1\le\gamma_v(P)+\delta c_2\\ 0; otherwise,\end{cases} \qquad (15)$$
$$B_n(c_2,c_1)=\begin{cases}1; if\ldots c_1>\gamma_n(P) and\ldots c_2>B(P)\\ 0; otherwise,\end{cases}$$
$$B_v(c_2,c_1)=\begin{cases}1; if\ldots c_1>\gamma_v(P)+\delta c_v and\ldots c_2\le B(P)\\ 0; otherwise\end{cases}$$

2.3 Discussion of the Results

By the observation of the derived equations it is clearly visible that a no-infection steady state equilibrium exists for P = 0.

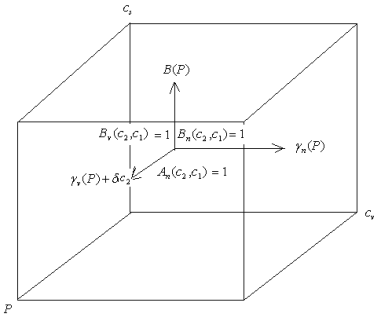

Figure 2: The optimal behavior of susceptible computers without AMS and their costs of being with AMS and self-hardening by steady state prevalence P

This steady state equilibrium is given by functions $A_n, B_v, B_n, C, S.I, V,$ and aggregate prevalence P. Figure 2 shows the steady state prevalence P for optimal behavior of susceptible computers without AMS and their costs of being with AMS and self-hardening.

3. CONCLUSION AND FUTURE DIRECTION TO THE WORK

An approach towards the use of utility cost of a computer being susceptible or infected is discussed in the paper. The write-up considers the role of AMS and the self-hardening action to find out the lifetime utility of a computer as these two are the major components to achieve the proactive defense. This lifetime utility is beneficial to take the decision, whether the self-hardening has to be implemented in the computer network or not as it is costly action to protect the computer network from malicious objects.

All the proportions of the total benefit B(P) has been derived in terms of the self-hardening cost and security cost of susceptible computers.

Initially, we assumed in the whole network all the computers are without AMS and no self-hardening. They are choosing these actions latter. So, an equilibrium is discussed among the possible combinations of susceptible computers who optimally choose to be either with an AMS or self-hardening or both for proactive defense, which is the final target of the paper. Future work at present is in the direction of giving its realistic implementation in the network.

4. REFERENCES

[1] Bimal Kumar Mishra, Dinesh Saini (2007), "Mathematical models on computer viruses", Applied Mathematics and Computation 187 (2007) 929–936

[2] Bimal Kumar Mishra, Dinesh Kumar Saini (2007), "SEIRS epidemic model with delay for transmission of malicious objects in computer network", Applied Mathematics and Computation 188 (2007) 1476–1482

[3] Hemraj Saini, Dinesh Kumar Saini (2007), "Malicious Objects Dynamics in the presence of Anti Malicious Objects", European Journal of Scientific Research 18(3) 491-499

[4] Hemraj Saini (2009), "Queuing Model for Malicious Attack Detection" , The Icfai University Journal of Information Technology 5(2) 16-28

[5] Hemraj Saini, Dinesh Kumar Saini (2008)," VAIN: A Stochastic Model for Dynamics of Malicious Objects" ICFAI journal of Systems Management 6(1) 14-28

[6] Lakkaraju, K. and Slagell, A. (2008), "Evaluating the utility of anonymized network traces for intrusion detection", In Proceedings of the 4th international Conference on Security and Privacy in Communication Netowrks (Istanbul, Turkey, September 22 - 25, 2008). SecureComm '08. ACM, New York, NY, 1-8. DOI= http://doi.acm.org/10.1145/1460877.1460899

[7] Michèle Cohen (2004), "Security level, potential level, expected utility: A three-criteria decision model under risk", Theory and Decision, Springer Netherlands 33(2) 101-134

[8] Hemraj Saini, Dinesh Kumar Saini (2007), "Proactive cyber Defense and Reconfigurable Framework of Cyber Security", International journal named International Review on Computer and Software, 2(2) 89-97

[9] Hemraj Saini, Dinesh Kumar Saini (2006), "CYBER DEFENSE ARCHITECTURE IN CAMPUS WIDE NETWORK", 3rd International Conference on Quality, Reliability and INFOCOM Technology (Trends and Future), Indian National Science Academy, New Delhi (INDIA), 2-4 December, 2006. Souvenir pp. 62

[10] Nick Clemente (2007), "System Hardening The Process of Defending and Securing Today's Information Systems", Journal of Security Education, 2(4) 89 – 118

[11] Yasuda, K. Kanazawa, T. (2003), "Proximate optimality principle based Tabu Search", Systems, Man and Cybernetics, 2003. IEEE International Conference on, vol.-2 1560- 1565

[12] Ross, S.: Introduction to Stochastic Dynamic Programming. Academic Press, New York(1983)