Optimal Operation of Information Security Systems: An Application of Anti-virus

WON SEOK YANG
Department of Business Administration
Hannam University
133 Ojung-dong, Daeduk-gu, Daejeon 306-791
SOUTH KOREA
wonsyang@hnu.kr

TAE-SUNG KIM
Department of Management Information Systems
Chungbuk National University
12 Gaeshin-dong, Heungduk-gu, Cheongju, Chungbuk 361-763
SOUTH KOREA
kimts@cbnu.ac.kr

Abstract: In this paper we analyze the operation of anti-virus software. We consider two types of operation policies: the real-time scan and the batch scan. Viruses arrive at the system according to a Poison process and receive the real-time scan. System managers update anti-virus software and apply the batch scan for the information system periodically. We derive the optimal batch scan interval to minimize the long-run average operating cost.

Key-Words: information security system, economic analysis, optimal operation policy, anti-virus

1 Introduction

As the side effects of information society, for example, virus, unauthorized access, theft of proprietary information, denial of access, etc., diffuse, the information security becomes one of the most important issues for organizations. According to a survey by CSI/FBI, total losses resulted by security attacks or misuse amount to about $130 million, and virus attacks alone resulted in about $43 million to 700 organizations in 2005 (CSI 2005). In response to these security threats, organizations have implemented several security counter-measures such as firewalls, anti-virus software, intrusion detection systems (IDS), encryption (of data in transit and of files), smart cards, etc. A major growing concern for organizations is to evaluate and compare the performance of portfolios consisting of security counter-measures.

Recently many researchers have studied on economic aspects of information systems security. The first group of the literature is on assessment of the economic benefits of information security investments. Gordon and Loeb (2002) provide an economic modeling framework for assessing the optimal amount to invest in information security to protect a given set of information. The second group is on the value of individual security technologies. Cavusoglu et al. (2005) assess the value of IDS in a firm's information technology security architecture. The third group is on guidelines for information security investment decision making. Cavusoglu et al. (2004) present an analytic model in an attempt to facilitate decisions regarding security investments. Bodin et al. (2005) show how a chief information security officer can apply the analytic hierarchy process (AHP) to determine the best way to spend a limited information security budget.

In this paper we suggest a probability model for the operation of anti-virus software. We derive a condition under which the operating policy is achieved. Some numerical examples with various cost structures are given to illustrate the results.

2 Model Description

We consider an information system where viruses arrive according to a Poisson process with rate λ. The information system has two types of anti-virus operation policies including 'real-time scan' and 'batch scan'. In the real-time scan policy, a virus is assumed to be scanned immediately after its arrival. Consequently, the real-time scan policy assumes infinite number of anti-viruses. We assume that the time for scanning and curing a virus follows a general distribution. In the batch scan policy, a system manager operates an anti-virus every deterministic time interval d and scan and cure all the viruses remaining in the system simultaneously.

The anti-virus operation policy considered in this paper is applicable to an information system with hundreds of personal computers connected through a network, for example, local area networks (LAN). Today, in an information system, every user has a copy of an anti-virus software in his or her PC and operates the anti-virus whenever he or she wants. The behavior of operating an anti-virus is different from person to person. That is, how often a user runs an anti-virus or how many files he or she scans might have different personal patterns. Therefore, a virus's survival time becomes stochastic. This corresponds to the real-time scan policy with stochastic operating time. On the other hand, system managers upgrade or update their anti-virus software periodically to deal with new types of viruses. After updating the anti-virus, they scan all the viruses in the system in order to protect their system from the damage caused by new viruses. This corresponds to the batch scan policy.

3 Cost Analysis

We consider a virus and an anti-virus for the real-time scan policy as a customer and a server in a queueing system, respectively. Note that the real-time scan policy assumes an infinite number of anti-viruses. Accordingly, the stochastic behavior of the model we consider is identical to the time dependent M/G/ ∞ queue until a system manager operates batch scan.

Let $G(x)$ be the cumulative density function of the operation time for the real-time scan and $Y(t)$ be the number of viruses scanned and cured by the real-time scan policy during $(0,t]$. From Gross and Harris (1974), we have the distribution function of $Y(t)$,

$$P[Y(t)=n]=\frac{[\lambda(1-q)t]^n e^{-\lambda(1-q)t}}{n!}\ ,\ \ n=0,1,2,\cdots \tag{1}$$

From (1), we have $E[Y(t)]$ as follows:

$$E[Y(t)]=\lambda(1-q)t \tag{2}$$

where q is given by

$$q=\int_o^t[1-G(x)]dx\Big/t.$$

In this paper, we seek to obtain the optimal time interval for the batch scan policy. So we focus on the cost analysis during the time interval d shown in Figure 1.

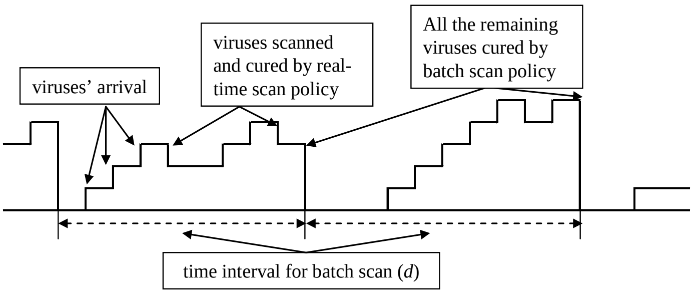
viruses' arrival
viruses scanned and cured by real-time scan policy
All the remaining viruses cured by batch scan policy
time interval for batch scan (*d*)

Figure 1. A Sample Path of the Model

Let c_R and c_B be the operation cost for the real-time scan and that for the batch scan per unit time, respectively. Let $C(d)$ be the long-run average operating cost during the time interval for the batch scan. Then, $C(d)$ can be expressed as

$$C(d)=\frac{c_B}{d}+c_R E[Y(d)] \tag{3}$$

Substituting (2) into (3), we obtain

$$C(d)=\frac{c_B}{d}+c_R\lambda\left(d-\int_o^d[1-G(x)]dx\right) \tag{4}$$

Let d^* be the optimal interval for batch scan which minimizes $C(d)$ in (4). Since $C(d)$ is a continuous and concave function, d^* is a value which makes the derivative of $C(d)$ become zero. Then, d^* is obtained by solving the following equation:

$$c_B\big/c_R=\lambda x^2 G(x) \tag{5}$$

Remark 1. Since d^* is the solution of the equation (5), c_B/d^* is identical to $c_R\lambda d^* G(d^*)$. c_B/d^* stands for the average cost during the optimal interval for the batch scan. And as $G(d^*)$ is the probability of finishing the real-time scan by d^*, $c_R\lambda d^* G(d^*)$ implies the average cost by the real-time scan.

Remark 2. The equation (5) shows that d^* depends only on the ratio of c_R and c_B. This result makes us easy to obtain d^* because we do not need to estimate c_R and c_B separately if we know their ratio.

4 Numerical Examples

We present numerical examples where the operation time for the real-time scan follows an exponential distribution with rate μ. That is, $G(x) = 1 - e^{-\mu x}$. In this case, the average long-run cost $C(d)$ is given by

$$C(d) = \frac{c_B}{d} + c_R \lambda d - \frac{c_R \lambda}{\mu}\left(1 - e^{-ud}\right)$$

And the optimal interval for batch scan, d^*, is given by solving the following equation:

$$\frac{c_B}{c_R} = \lambda x^2 [1 - e^{-ux}] \qquad (6)$$

First, we present the shape of the average cost $C(d)$ over the interval for the batch scan. In Figure 2, the average cost shows a continuous and concave function and has one global optimal solution as we mentioned above.

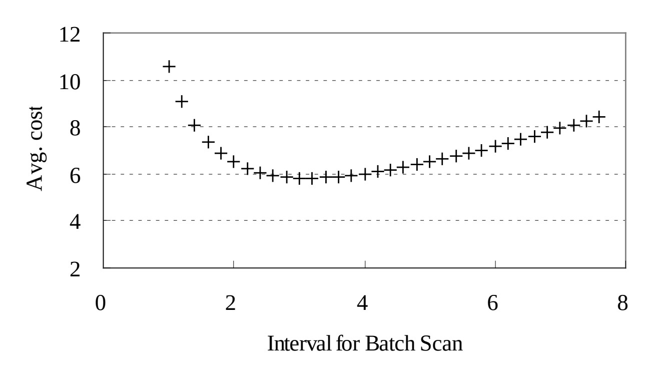

Figure 2. Average Cost

The optimal value d^* is 3.2 where $\lambda = 1$, $\mu = 2$, $c_R = 1$, and $c_B = 10$ in Figure 2.

Now, we examine the average costs where the ratios c_B/c_R stay constant. We analyze four cases having the cost structures shown in Table 1 with different values for c_R and c_B but the same value for the ratio c_B/c_R.

Table 1. Cost Structure A

Items	Case 1	Case 2	Case 3	Case 4
c_B	20	15	10	5
c_R	4	3	2	1
c_B/c_R	5	5	5	5

Figure 3 gives the analysis results of the above four cases in Table 1. Figure 3 shows that the optimal interval for the batch scan, d^*, has the same value for each case. This result confirms what we mentioned in Remark 1. In Figure 3, we assumed that $\lambda = 1$ and $\mu = 2$. Then, the optimal value d^* is 2.2.

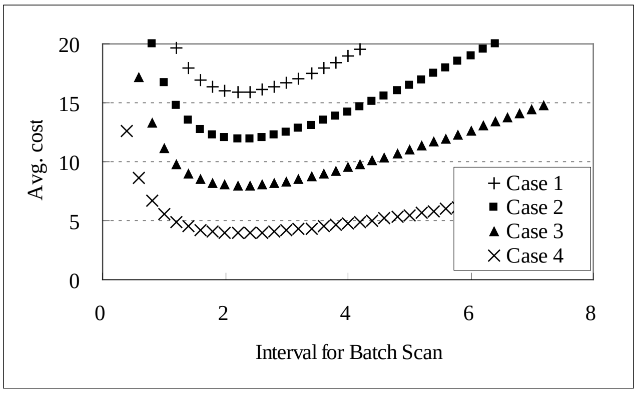

Figure 3. Average Cost with the Same Value for c_B/c_R

Next, Figure 4 presents examples with different values of c_B/c_R shown in Table 2.

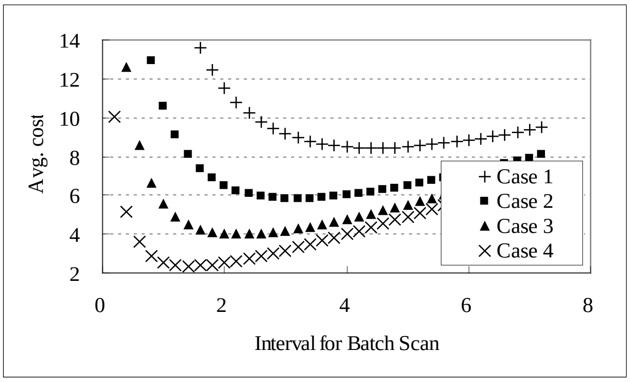

Figure 4. Average Cost with Different Values for c_B/c_R

Table 2. Cost Structure B

Items	Case 1	Case 2	Case 3	Case 4
c_B	20	10	5	2
c_R	1	1	1	1
c_B/c_R	20	10	5	2

Figure 4 shows that d^* increases over the ratio c_B/c_R of which results are summarized in Figure 5. We obtain the optimal values d^* by solving the equation (6) numerically.

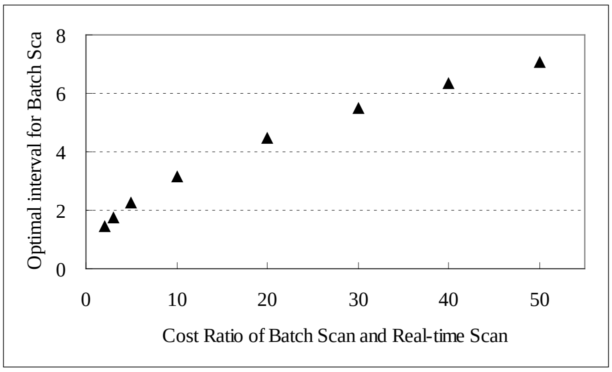

Figure 5. The Optimal Interval for Batch Scan over c_B/c_R

Now, we examine the average cost over the arrival rate of viruses λ with the fixed value of μ, the operation rate of the real-time scan, shown in Table 3. We assume that $c_B = 20$ and $c_R = 1$.

Table 3. Arrival Rate of Viruses

Items	Case 1	Case 2	Case 3	Case 4
λ	8	6	4	2
μ	10	10	10	10

Figure 6 shows the higher average cost for the higher values of λ. The optimal interval for the batch scan increases as λ decreases with the fixed value of μ.

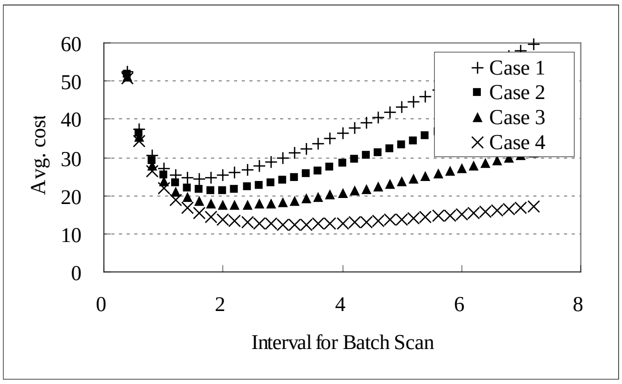

Figure 6. The Average Cost over the Arrival Rates of Viruses

5 Conclusions

In this paper we analyzed the operation of anti-virus software, and derived the optimal batch scan interval. With numerical examples, various cost structures were compared on the basis of the long-run average operating cost. We expect the analysis results and the numerical examples to help the system managers decide the operating policy.

Analyses for the economic operation of other major information security counter-measures such as firewalls, IDS, encryption, smart cards, etc can be suggested for the future research.

References:

[1] Bodin, L.D., L.A. Gordon and M.P. Loeb, "Evaluating information security investments using the Analytic Hierarchy Process," Communications of the ACM, vol. 48, pp. 79-83, 2005.

[2] Cavusoglu, H., B. Mishra and S. Raghunathan, "A model for evaluating IT security investments," Communications of the ACM, vol. 47, pp. 87-92, 2004.

[3] Cavusoglu, H., B. Mishra and S. Raghunathan, "The value of intrusion detection systems in information technology security architecture," Information Systems Research, vol. 16, pp. 28-46, 2005.

[4] Computer Security Institute, CSI/FBI Computer Crime and Security Survey, 2005.

[5] Gordon, L.A. and M.P. Loeb, "The economics of information security investment," ACM Transactions on Information and Systems Security, vol. 5, pp. 438-457, 2002.

[6] Gross, D. and G.M. Harris, Fundamentals of Queueing Theory, John Wiley & Sons, New York, 1974.