Catch Thieves Online: IT Security

Zhao Qian
Su Xueyuan
Song Yunji
University of Electronic Science and Technology
Chengdu, Sichuan, China

Advisor: Du Hongfei

Summary

We construct an optimal defensive system for IT security for a university network. After estimating whether the security measures' effect is worth the expense, we develop a model to seek the minimum sum of opportunity costs and defensive system expense.

The model is composed of three modules.

- Module 1 mainly deals with the risk evaluation. We apply the Analytic Hierarchy Process (AHP) to clarify the miscellaneous risks and separate the complex university network into nine simple subsystems.
- Module 2 employs a fast search algorithm to determine a technological defensive system for each subsystem.
- Module 3 determines the policies for the whole university network system and calculates the total cost.

By using our model, we cut down the expense from an initial \$8.9 million to \$3.4 million. At the same time, this model is flexible enough to adapt to changing technological capabilities and can be applied to different organizations. Although the model has strengths such as modularization, high efficiency, and flexibility, it is a pity that we can only play defense—we do not have the initiative. If we want to change that fact, we urgently need new technologies, such as honeynets.

The UMAP Journal 25 (2) (2004) 157–169.

Introduction

Risks to IT security can be broken down into the three categories of confidentiality, integrity, and availability; hence, we face a problem in multiple-objective programming. Risk evaluation is very complex; there are not only quantitative standards of evaluation, but also qualitative standards that are difficult to measure. At the same time, the evaluation is affected by people's economic ideas, so a benchmark cannot be easily determined. In addition, the task of evaluation is dynamic, since it changes with the development of society. Hence, what we should do is analyze the cost and estimate whether the security system's effect is worth the expense. After the risk evaluation, we can set up a defensive system that balances the opportunity costs and the defense system expense, minimizing the total cost.

Assumptions

- Any complex computer network system can be separated into several unrelated subsystems by different functions. For example, the bookstore and the registrar's office are two different subsystems of a university.
- Different defensive measures play different roles in IT security system. For example, a network-based firewall and a host-based firewall perform different functions.
- Each new defensive measure has been evaluated before being made available; so we can use a new defensive measure in our model directly, because its effect is known.
- New defensive measures can only decrease the loss due to the aging of old defensive measures.

Table 1.
Symbol table.

Symbol	Meaning
T	Total cost of the whole network defensive system
c	Opportunity cost contributed by the Confidentiality risk
i	Opportunity cost contributed by the Integrity risk
a	Opportunity cost contributed by the Availability risk
d	Defensive expense, including procurement, maintenance, and system administrator training costs
T_j	Total cost for subsystem j
c_j	Confidentiality risk cost for subsystem j
i_j	Integrity risk cost for subsystem j
a_j	Availability risk cost for subsystem j
d_j	Defensive expense for subsystem j

Dealing with the Data

Enclosures A and B describe the technology and policy preventive defensive measures. The information was obtained by interviewing consumers, who gave each measure a rating. The data are summarized in terms of Low (minimum), Mean, and High (maximum) values, together with Variability (indicating the concentration of the data about the Mean), which is recorded as Low, Med, or High.

We need to determine a single value for each measure:

- If the Variability is Low, the opinions of different consumers are almost the same. We use the Mean value.
- If the Variability is Med, we assume that 10% gave the Low value, 10% the High value, and the rest the Mean. We calculate the value of the measure as

$$\text{Value} = 0.10 \times \text{Low value} + 0.80 \times \text{Mean value} + 0.10 \times \text{High value}.$$

- If the Variability is High, we assume that 20% gave the Low value, 20% the High value, and the rest the Mean. We calculate the value of the measure as

$$\text{Value} = 0.20 \times \text{Low value} + 0.60 \times \text{Mean value} + 0.20 \times \text{High value}.$$

Although the specific numerical values of 10% and 20% may not be suitable for all cases, the specific values in fact will not affect the models that we develop.

Optimal Defensive Measures for a University

If there are no defensive measures, the opportunity cost projection is as shown in **Table 2** and the total cost is

$$T = 3.8 + 1.5 + 2.9 + 0.4 + 0.08 + 0.25 = \$8.93 \text{ million}.$$

The initial Confidentiality risk cost is

$$c = 3.8 \times 0.55 + 1.5 \times 0.70 + 2.9 \times 0.40 = \$4.3 \text{ million}.$$

Analogously, the initial Integrity risk cost and the initial Availability risk cost are

$$i = \$3.585 \text{ million}, \qquad a = \$1.045 \text{ milliion}.$$

Each defensive measure affects four factors: User Productivity, Confidentiality, Integrity, and Availability. However, the cumulative effects within and between the risk categories cannot just be added. Hence, we shift our focus from the effect on the four factors to the effect on the costs. For example, from an

Table 2.

Current opportunity costs and risk Category contributions (data from the problem statement).

Symbol	Opportunity Cost (due to IT)	Amount ($ millions)	Risk Category Contribution		
			C	I	A
P1	Litigation	3.8	55%	45%	
P2	Proprietary data loss	1.5	70%	30%	
P3	Consumer confidence	2.9	40%	30%	30%
P4	Data reconstruction	0.4		100%	
P5	Service reconstruction	0.08		100%	
P6	Direct revenue loss	0.25		30%	70%

initial Confidentiality opportunity cost of $10,000, a factor value of 25% would increase the Confidentiality level by 25% and at the same time result in a new Confidentiality opportunity cost of $\$10,000 \times (1 - 0.25) = \$7,500$. Thereby, improvements attributable to specific measures are directly associated with decreases in costs. Moreover, costs can be added directly.

Based on such ideas, we consider the effects of different defensive measures in economic terms. Our task can be described as structuring an optimal network defensive system to minimize the total cost $T = c + i + a + d$, where c, i, and a are potential opportunity costs and d is expense on defensive measures.

We organize our model into three modules. Each module completes a specific task:

- Module 1 separates the whole university network system into several subsystems by different functions. After analysis of these subsystems, the initial opportunity cost is distributed among the subsystems. Hence the aim of our task becomes to find
$$\min T = \sum_j T_j.$$
- Module 2 determines the technological measures used for each subsystem to minimize the cost of the subsystem, that is, for subsystem j the task is to find
$$\min T_j = c_j + i_j + a_j + d_j.$$
- Module 3 determines the policies for the whole university network system and calculates the total cost.

Module 1: Apply AHP to Subsystems

The university's various components have different functions and hence different requirements for Confidentiality, Integrity, and Availability. So based on the structure and functions of the network, we separate the whole university network system into nine subsystems (**Figure 1**), designated A1–A9 in **Table 3**.

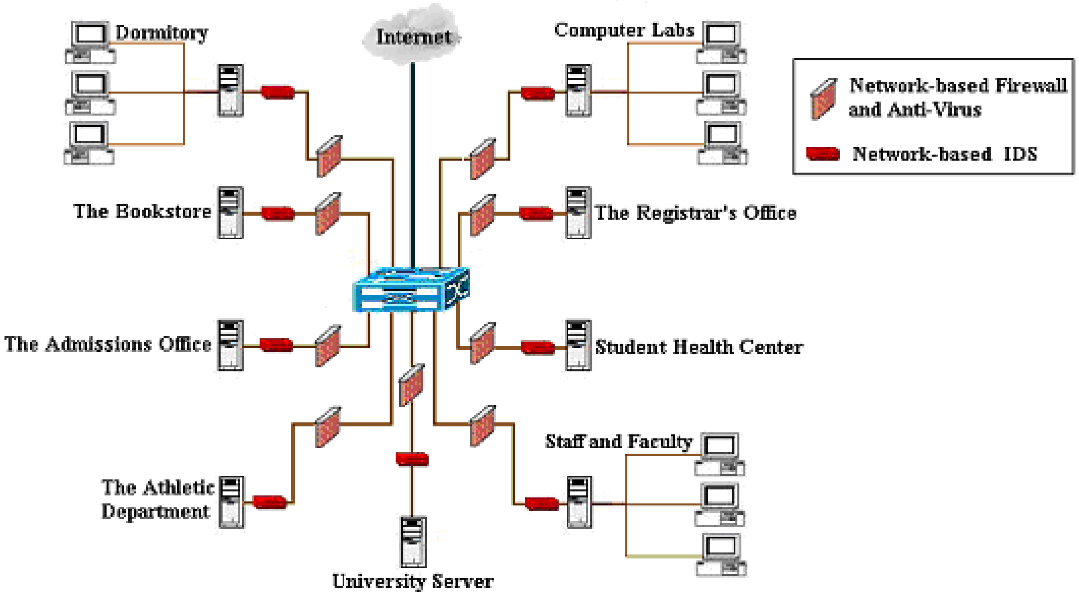


Figure 1. Separation of the network system.

Table 3.
Subsystems of the university network system.

Symbol	Subsystem
A1	Computer Labs
A2	Staff and Faculty Computers
A3	Dormitory Network
A4	Bookstore
A5	Registrar's Office
A6	Admissions Office
A7	Student Health Center
A8	Athletic Department
A9	University Server

We install a set of defensive systems for each subsystem. Such a defensive system defends against attacks on just that particular subsystem, so the cost of each subsystem can be calculated separately. We distribute the initial opportunity cost among the subsystems. We determine the weights for the subsystems by application of the Analytic Hierarchy Process (AHP) [Saaty 1980], a way to evaluate systems that involves both quantitative analysis and qualitative analysis. It exhibits the analytic and synthetic thoughts in decision-making strategy.

The hierarchy of the system is shown in **Figure 2**; A1–A9 stand for the nine subsystems in **Table 2** and P1–P6 represent the six kinds of opportunity costs in **Table 1**.

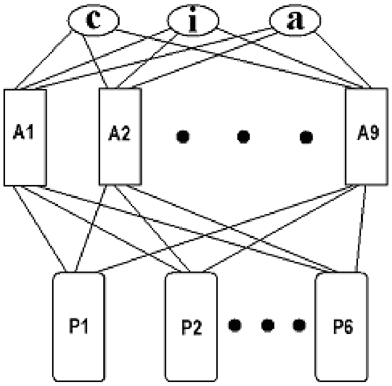


Figure 2. Hierarchy of the network system.

Our aim is to determine the weights for the risk categories distributed into each subsystem. As an example, we describe the calculation for the Confidentiality risk cost c. **Figure 3** shows the detailed c branch.

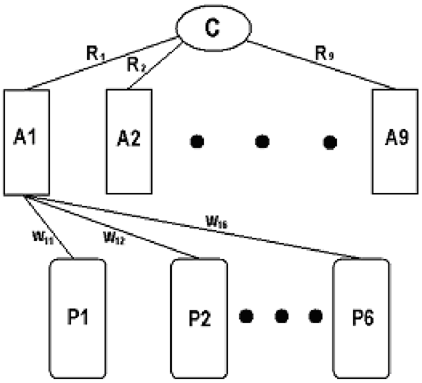


Figure 3. Detailed c branch.

We set up the equation

$$WR = T,$$

or

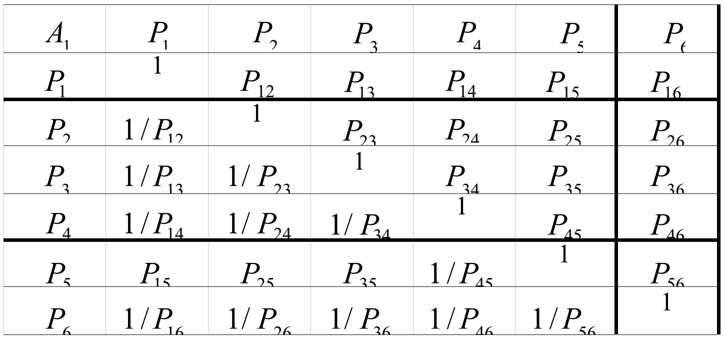
$$\begin{pmatrix} w_{11} & \dots & w_{91} \\ \vdots & & \vdots \\ w_{91} & \dots & w_{96} \end{pmatrix} \begin{pmatrix} R_1 \\ \vdots \\ R_9 \end{pmatrix} = \begin{pmatrix} t_1 \\ \vdots \\ t_6 \end{pmatrix}.$$

The elements w_{mn} are the weights of the six kinds of opportunity costs in each subsystem, where m is the subsystem and n is the kind of opportunity cost. For example, $w_{34} = P_4/c_4$ in subsystem A3, that is, w_{34} = (Data reconstruction loss)/(Confidentiality risk cost) in the dormitory network.

The elements R_m are the weights of the nine subsystems in risk categories. For example, $R_3 = c_3/c$.

The elements t_n are the weights of the six kinds of opportunity costs in the whole system. For example, $t_4 = P_4/c$, that is, t_4 = (Data reconstruction loss)/(Confidentiality risk cost) in the whole system.

Based on the analysis of the functions of each subsystem, we develop nine judging matrices to analyze the weight of each subsystem. Take A1 (Computer Labs), for example: The element P_{mn} represents the importance of P_m to P_n.



A_1	P_1	P_2	P_3	P_4	P_5	P_6
P_1	1	P_{12}	P_{13}	P_{14}	P_{15}	P_{16}
P_2	$1/P_{12}$	1	P_{23}	P_{24}	P_{25}	P_{26}
P_3	$1/P_{13}$	$1/P_{23}$	1	P_{34}	P_{35}	P_{36}
P_4	$1/P_{14}$	$1/P_{24}$	$1/P_{34}$	1	P_{45}	P_{46}
P_5	P_{15}	P_{25}	P_{35}	$1/P_{45}$	1	P_{56}
P_6	$1/P_{16}$	$1/P_{26}$	$1/P_{36}$	$1/P_{46}$	$1/P_{56}$	1

Commonly, we use 1, 2, 3, . . . , 9 and their reciprocals to represent different degrees of importance: The larger the number, the more important the factor. While P_{mn} represents the importance of P_m to P_n, the importance of P_n to P_m is $1/P_{mn}$.

We normalize the column vectors in the judging matrix,

$$\overline{P_{mn}} = \frac{P_{mn}}{\sum_{k=1}^{6} P_{kn}},$$

and then add the normalized matrix in rows:

$$\overline{W_{mn}} = \sum_{k=1}^{6} \overline{P_{kn}}.$$

We normalize again to get

$$w_m = \frac{\overline{W_m}}{\sum_{k=1}^{6} \overline{W_k}},$$

The eigenvector w represents the opportunity costs' weights in the subsystem. Use the judging matrix P and eigenvector w, we calculate the maximum eigenvalue

$$\lambda_{\max} = \sum \frac{(PW)_m}{6W_m},$$

where $(PW)_m$ is the mth element of the vector Pw obtained as the product of the matrix P and the vector w.

Last, we check the coherence of the judging matrix. For a six-row matrix, the standard of coherence, CI, is calculated as

$$\text{CI} = \frac{\lambda_{\max} - 6}{5},$$

and if CI < 0.124, then the coherence of the judging matrix is suitable; otherwise, the judging matrix needs to be adjusted.

Following the approach indicated, we calculate the eigenvector of each subsystem's judging matrix and combine them into matrix W to get

$$W = \left(\begin{matrix} 0.2756 & 0.0795 & 0.0795 & 0.4817 & 0.0502 & 0.0335 \\ 0.4290 & 0.2093 & 0.2093 & 0.0817 & 0.0415 & 0.0291 \\ 0.4606 & 0.0429 & 0.3384 & 0.0724 & 0.0429 & 0.0429 \\ 0.1057 & 0.0638 & 0.5650 & 0.0638 & 0.0396 & 0.1621 \\ 0.4334 & 0.2147 & 0.2147 & 0.0640 & 0.0433 & 0.0299 \\ 0.2463 & 0.1252 & 0.4579 & 0.0569 & 0.0294 & 0.0843 \\ 0.4547 & 0.2440 & 0.1771 & 0.0349 & 0.0349 & 0.0544 \\ 0.0949 & 0.0581 & 0.5641 & 0.1528 & 0.0949 & 0.0378 \\ 0.4455 & 0.1604 & 0.2306 & 0.0800 & 0.0288 & 0.0547 \end{matrix}\right.$$

For the matrix T, we get

$$T = (0.4406 \;\; 0.2238, \;\; 0.2238 \;\; 0.0373 \;\; 0.0373 \;\; 0.0373)^T.$$

We calculate R as

$$R = W^{-1}T.$$

Two conditions must be fulfilled:

- The elements in matrix R must be nonnegative.
- The sum of the elements in R must equal 1.

Some adjustments may be needed to fulfill the conditions. At last, we get

$$R = (0.1674 \;\; 0.0435 \;\; 0.0000 \;\; 0.1915 \;\; 0.6120 \;\; 0.5364 \;\; 0.0000 \;\; 0.0000)^T.$$

The process described above is for the Confidentiality risk cost (c). The results for all opportunity costs are shown in **Table 4**.

Table 4.
Distribution details of opportunity costs.

	A1	A2	A3	A4	A5	A6	A7	A8	A9
c	0	16.74%	4.35%	0	19.15%	6.12%	53.64%	0	0
i	11.04%	9.84%	43.24%	0	0	0	18.91%	0	16.97%
a	0	0	0	73.18%	0	0	0	26.82%	0

From **Table 4**, we can know the distribution of initial opportunity costs among subsystems. For example, for A1 (Computer Labs), the Integrity risk cost is

$$i_1 = \$3.585 \text{ million} \times 11.04\% = \$0.395 \text{ million}.$$

With the distribution of initial opportunity costs among subsystems now available, we can determine the defensive system for each subsystem.

Module 2: Perform a Fast Search Algorithm

Defensive measures include technologies and policies. Technologies are hardware and software installed to protect the network; policies are guidelines publicized to instruct users' activities. Technologies should be different in each subsystem, according to the function it realizes; but policies should be the same throughout the whole network system.

Technologies

Technologies consist of host-based firewall (HF), network-based firewall (NF), host-based anti-virus (HA), network-based anti-virus (NA), network-based intrusion detection system (IDS), spam filter (SPAM), network-based vulnerability scanning (NVS), data redundancy (DR), and service redundancy (SR). We need to structure these technologies into several defensive layers.

Firewalls defend against attack from hackers, while anti-virus protects the server from the virus. Their effects must be considered together, since they form one defensive layer.

SPAM filtering, vulnerability scanning, data redundancy, and service redundancy are not real-time technologies. The form another defensive layer.

The defensive layers are shown in **Figure 4**.

The configurations of each subsystem are the same; the difference lies in which measure should be chosen in each defensive layer. Hence, the search process is the same for each subsystem. We describe our fast search algorithm:

1. For the first layer, we search the measure to minimize the total cost, finding a locally optimal solution.

2. We go on to the next layer. Based on the result of the previous layer, we combine the effects of different measures in this layer to find another locally optimal solution.

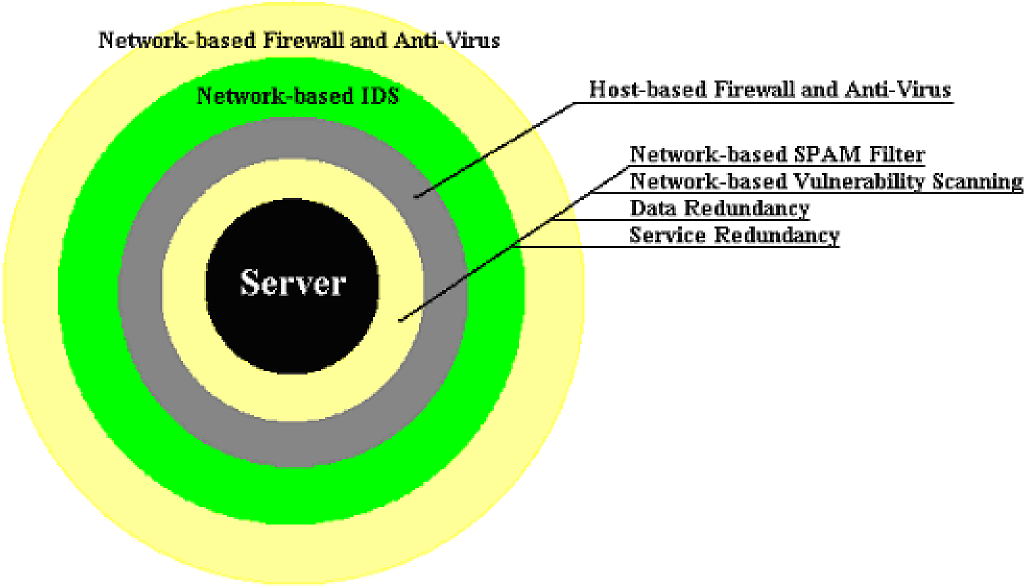

Network-based Firewall and Anti-Virus
Network-based IDS
Host-based Firewall and Anti-Virus
Network-based SPAM Filter
Network-based Vulnerability Scanning
Data Redundancy
Service Redundancy
Server

Figure 4. Technologies defensive layers.

3. Iterate Step 2 until all four defensive layers have been examined.
4. If all the measures of a technology cannot cut down the cost, it means that this technology is not needed. After the iterative search, the locally optimal solution will approach the globally optimal solution at last.

Following the search algorithm, we determine the technological measures suitable for each subsystem. The result is shown in **Table 5**.

Table 5.

Technological measures for each subsystem.

	NF	NA	IDS	HF	HA	SPAM	NVS	DR	SR
A1	2	2	8	1	1	0	0	0	4
A2	2	2	8	1	2	0	0	0	4
A3	2	2	8	1	1	0	0	0	4
A4	3	2	9	7	3	1	0	0	4
A5	2	3	9	1	2	0	0	0	0
A6	2	3	9	1	2	0	0	0	0
A7	2	2	2	1	2	0	0	0	4
A8	3	2	9	7	3	0	0	0	4
A9	2	2	8	1	1	0	0	0	4

This table shows the optimal defensive systems for each subsystem. The numbers in the table represent the sequence number of measures in each technology. For example, for A1 (Computer Labs), we choose the 2nd measure (Network defense) for Network-based Firewall and 8th measure (Network eye) for Network-based Intrusion Detection System. Note that 0 means that none of the measures of such technology is suitable, so this technology is not needed for the subsystem; for example, SPAM, NVS, and DR are not needed for A1.

Using the technological measures in **Table 5**, we calculate the effect of such measures for each subsystem. By adding such effects, we get the effect for the whole system (**Table 6**).

Table 6.
Effects of technologies (in millions of dollars).

	c	i	a		Total
Initial opportunity cost	4.3	3.6	1.0		8.9
Opportunity cost after technology defenses	1.5	1.0	0.4		
plus cost in technologies				0.5	3.4

Module 3: Determine the Policies

Policies to instruct users' activities should be the same throughout the whole network system. There are seven kinds: Passwords, Formal Security Audits, Wireless, Restrict Removable Media, Personal use, User Training and Sys Admin Training.

We check the effect of each policy by following the search algorithm that we used in Module 2. The result is shown in **Table 7**.

Table 7.
Policies for the network system.

Area	Policy
Password	Strong
Formal Security Audits	No need
Wireless	Disallow
Restrict Removable Media	No restriction
Personal Use	Unmonitored
User Training	Needed
Sysadmin	No need

The economic effect of this set of policies, after adoption of the technologies prescribed, is shown in **Table 8**.

Table 8.
Effects of policies (in millions of dollars), after adoption of recommended technologies.

	c	i	a		
Opportunity cost before policies	1.5	1.0	0.4		2.9
Opportunity cost after policies	0.8	0.5	0.2		
plus cost of policies				1.3	2.9

In all, the effect of the recommended defensive system is shown in **Table 9**.

Table 9.
Effect of the whole defensive system (in millions of dollars).

	c	i	a	d	Total
Cost with no defensive system	4.3	3.6	1.0	0	8.9
Cost under recommended defensive system	0.8	0.5	0.2	1.8	3.4

The minimized total cost is

$$T = c + i + a + d = 0.8 + 0.5 + 0.2 + 1.8 = \$3.4 \text{ million.}$$

Updating the IT Security System

Every organization has a potential opportunity cost that can be broken down into the three categories of Confidentiality, Integrity and Availability, which costs we choose as parameters. Additionally, the model separates the whole network system into subsystems by network structure and functions. These issues do not change in different organizations. So this model has a universal character and can be used in defensive system design for all kinds of organizations.

At the same time, technical specifications change over time. With the progress of technology, new attack measures are taken by hackers, and our security system will lose its power. Hence, we should update the security system regularly. But two questions lie before us:

- Which kind of new technology do we need?
- How often should we update the security system?

To answer the questions, we assume that the effect of all technologies decreases periodically and new technologies appear at the same time. Based on these assumptions, we describe our measure as follows:

- The first technology to replace is the one with the poorest effect.
- The time to update the system is not fixed but is based on the current security system's state and the capability of the new technology.
- We evaluate the cost when new technology appears. If the application of new technology can decrease the total cost further, then the old technology should be replaced.

We take the bookstore (A4) as an example to describe our approach. From the earlier result, we know that the opportunity cost of the bookstore is $.7318 \times \$1{,}045{,}000 = \$765,000$, all of it contributed by Availability (**Table 1**). Hence, when new technology appears, only the effect on availability should be taken into consideration. Suppose that every month a new kind of host-based firewall appears and the effect on availability of the firewall in use decreases by 3%. With the rapid decrease of effect, host-based firewall becomes the weakness of the security system.

- Suppose that the security system of the bookstore is established in April. The host-based firewall in use is "watertight" and its effect on availability is 19.4%.

- In May, the effect reduces to 16.4%. If there were no firewall, the opportunity cost of the bookstore would be $16,839 this month. Firewalls defend against attack from hackers, while antivirus protects the server from viruses, so their effects are additive. We assume that firewalls and antivirus protects each have 50% of the protective effect, so the current firewall reduces the opportunity cost by $\$16, 839 \times .164 \times 50\% = \$1{,}381$. At the same time, a new host-based firewall appears whose effectiveness on Availability is 20.3%, while it costs $1,045 to install. If the new firewall is installed, considering the installation cost, it reduces the opportunity cost by $\$16{,}839 \times .102 - \$1{,}045 = \$1{,}709 - 1{,}045 = \$664$. It is clear that keeping the old firewall is more suitable.

- Things change again in June. Since the effect of the original firewall reduces to 13.4%, it can cut down the cost by only $1,128. In this month, another new host-based firewall appears; assume that its effectiveness on Availability is 19.2%, while it costs $1,015 to install. So, the application of the new firewall reduces the cost by $1,617 − $1,015 = $602. It is still not worth the expense.

- In July, we again evaluate the opportunity cost. The effect of the original firewall is 10.4%, so it can save just $876. The effect of the new firewall is 23%, and it costs $1,045 to install. The application of the new firewall saves $1,937 − $1,045 = $892. With the new firewall, we can save $16 more. So we should update the firewall in July.

References

Brin, Sergey, and Lawrence Page. 2000. The anatomy of a large-scale hypertextual Web search engine. `http://www-db.stanford.edu/~backrub/google.html` .

Curtin, Matt. 1998. Introduction to network security. `http://www.interhack.net/pubs/network-security/network-security.html` . Last revised 16 July 1998.

Honeynet Project. 2003a. Know your enemy: Honeynets—What a honeynet is, its value, how it works, and risk/issues involved. `khttp://project.honeynet.org/papers/honeynet/index.html` . Last modified 12 November 2003.

Honeynet Project. 2003b. Know your enemy: Defining virtual honeynets: Different types of virtual honeynets. `http://www.honeynet.org/papers/virtual/` . Last modified 27 January 2003.

Mitra, Sanjit Kumar. 2001. *Digital Signal Processing: A Computer-Based Approach*. 2nd ed. New York: McGraw-Hill.

Oppenheim, Alan V., and Alan S. Willsky. 1996. *Signals and Systems*. 2nd ed. Englewood Cliffs, NJ: Prentice-Hall.

Saaty, T.L. 1980. *The Analytic Hierarchy Process.* New York: McGraw-Hill.