J Inf Process Syst, Vol.16, No.1, pp.61~82, February 2020
https://doi.org/10.3745/JIPS.02.0128

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

A Cost-Optimization Scheme Using Security Vulnerability Measurement for Efficient Security Enhancement

Jun-Young Park[*] and Eui-Nam Huh[*]

Abstract
The security risk management used by some service providers is not appropriate for effective security enhancement. The reason is that the security risk management methods did not take into account the opinions of security experts, types of service, and security vulnerability-based risk assessment. Moreover, the security risk assessment method, which has a great influence on the risk treatment method in an information security risk assessment model, should be security risk assessment for fine-grained risk assessment, considering security vulnerability rather than security threat. Therefore, we proposed an improved information security risk management model and methods that consider vulnerability-based risk assessment and mitigation to enhance security controls considering limited security budget. Moreover, we can evaluate the security cost allocation strategies based on security vulnerability measurement that consider the security weight.

Keywords
Attack Graph, Cloud Security, Cost Optimization, Vulnerability Measurement

1. Introduction

With the new development of information communication technologies (ICTs), such as autonomous vehicles, drones, and artificial intelligence, modern life is becoming increasingly convenient in nearly all areas of life. ICT is not only adopted for improving the quality of life; industry fields are also trying to introduce new ICTs with Industry 4.0. According to the threat report of THALES [1], a global security company, 63% of respondents among 1,100+ senior security executives described that their organizations apply new technologies without considering levels of security. The report shows that development of ICT without considering security technology might cause irreversible security incidents. Therefore, we need to consider security for safer ICT environments.

Most companies and organizations are trying to improve their ICT security environment and increase security budget annually [2]. However, not all efforts that are allocated in the security cost are effective. According to a survey report [3], the ICT security budget is decided by boards of directors and C-level executives who lack expertise and knowledge about ICT security, and 81% of respondents and 42% of the IT security practitioners replied that the ICT security budget is less than adequately allocated.

Manuscript received April 12, 2018; first revision July 24, 2018; second revision October 31, 2018; accepted April 22, 2019.

Corresponding Author: Eui-Nam Huh (johnhuh@khu.ac.kr)
* Dept. of Computer Science and Engineering, Kyung Hee University, Yongin, Korea (parkhans@khu.ac.kr, johnhuh@khu.ac.kr)

Moreover, 53% of respondents rate their organization's annual budgeting process for IT security activities as complex, and only 32% of respondents say the budget is appropriate based on an assessment of our organization's security risks. For these reasons, we need systematic information security risk management methods for efficient security risk management.

For systematic and efficient security risk management, we need to understand information security risk management [4] by priority. The security cost allocation, one of the risk treatment methods in information security risk management, is determined based on risk assessment. Therefore, we should consider risk assessment, risk treatment, monitoring, and review for security enhancement.

The security risk assessment methods consist of qualitative methods and quantitative methods. In Table 1, we summarize major risk assessment methods for information security [5].

Table 1. Major information security risk assessment methods

Risk evaluation method		Main metric
Qualitative	OCTAVE	Loss = Impact/consequence * Probability
	CORAS	Loss = Impact * Probability
Quantitative	ISRAM	Risk = Probability of OSB * Consequence of OSB
	CORA	ALE = Consequence * Frequency
	RiskWatch	Risk = Frequency of a threat in a year * Cost of the resource

OSB=occurrence of security breach.

Recently, existing risk assessment methods have tended to center around the probability and damage using assessment factors such as frequency of threats, asset consequence, cost of the resource, etc. However, the target of security risk assessment should be a security vulnerability according to the attack paths [6-8] of Open Web Application Security Project (OWASP), as shown in Fig. 1.

The attack flow defined by OWASP starts with attacks of attackers on vulnerabilities of service providers. An attack using a vulnerability should be prevented or mitigated though a security control, and if it passes the security control, a technical or business impact occurs. Therefore, to enhance security, the vulnerabilities are minimized by improving a related security control. Moreover, the security threats consist of one or more security vulnerabilities, which should be taken into account in terms of systematic or continuously attacks security vulnerabilities. For the reason, the security vulnerabilities should evaluate rather than security threats.

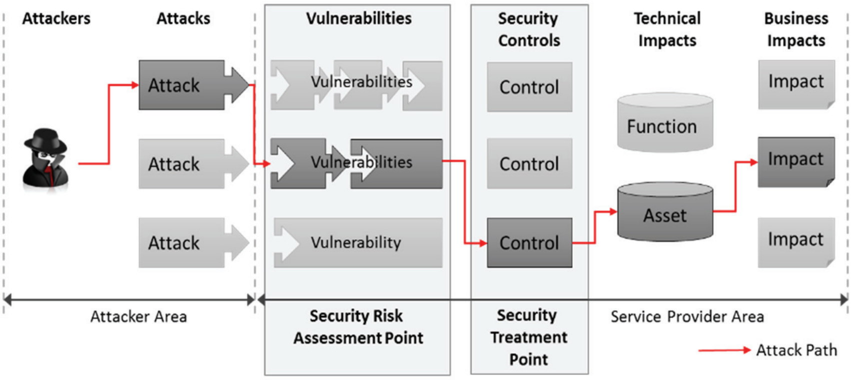


Fig. 1. OWASP attack flow.

Additionally, some threat-oriented security risk assessment can be evaluated in duplicate of the same threats among security attack techniques. For example, data breach and data loss are different security threats. However, both threats have the same security vulnerability such as hijacking administrator accounts. Thus, existing security evaluation methods have the problem of repeatedly evaluating the same security vulnerability based on different security threat. Therefore, we need an accurate security risk assessment method based on vulnerability without duplicate risk evaluation.

Existing security cost optimization methods [4,9,10] are aimed at calculating the security budget considering security environment or maximizing benefit. However, as shown in Fig. 2, the security control performs activities in order to prevent or mitigate security attacks based on vulnerabilities. Therefore, it should be a security cost allocation considering each security control rather than calculating the total security budget for strengthening security. In addition, the importance of security control is different depending on the characteristics of the provided service. Therefore, the security cost optimization strategies should be determined by considering the weight in the security control according to the provided service. Finally, according to [2], most companies determine their security budget within 3% of their overall budget. However, since the existing security cost optimization methods do not consider the limited security budget but only calculate the optimal allocation budget for security enhancement effect, a method for optimum security cost allocation on a limited budget is needed.

This paper is organized as follows: In Section 2, related methods are examined. In Section 3, the proposed security cost optimization model is explained. Section 4 describes the simulation of the proposed method. Finally, Section 5 presents the conclusions of this research.

2. Related Works

As mentioned in the introduction, Security risk evaluation should be conducted as vulnerability-based security evaluations rather than threat and impact-based evaluation, such as OWASP attack flow. Recently, attack graphs [11,12] have been most commonly used for security evaluation based on security attacks such as Attack Tree [13,14] and Attack Defense Tree [15,16]. The attack graph lists the vulnerabilities of attack/threat to reach the attack target and helps specify the optimal attack route. However, attack graphs and trees address only one attack goal and do not consider correlation between attack nodes. We need to consider all of the potential attacks against the security in an attack perspective.

In an optimized security cost scheme, we need to consider the minimization of security vulnerability or asset/business impact based on the weight of security control with regard to service type. To define the weight of security control according to service type, we refer to several decision-making methods such as the analytic hierarchy process (AHP) and the Delphi method [17]. Tian et al. [18] suggested a novel threat evaluation model using the AHP, and Na et al. [19] proposed a definition of weight security control according to service type using the AHP.

The purpose of most security enhancement schemes [20-22] is to propose a cost optimization scheme for the best benefit. These schemes have been researched and applied in many companies and the IT industries in [22]. Unfortunately, most these schemes do not take into account characteristics of various computing environments or target services.

In addition, each of these schemes consider different elements when determining security cost allocation. Most these schemes use two basic elements: the probability of an event occurring and the losses that this may incur. This is called the expected annual loss (ALE) or estimated annual cost (EAC). These elements are calculated for an event by simply multiplying the probability of potential losses.

We can predict the benefit of any cost allocation strategies using return on investment (ROI) or return on security investment (ROSI) [23] based on ALE. This shows loss variation between before and after cost allocation. Recently, most security cost allocation researches using ROSI have been introduced [23-25]. However, it is difficult to calculate ALE and risk mitigation value. Therefore, we need a systematic security cost optimization model based on a vulnerability analysis.

According to [3], ROSI and TCO (total cost of ownership) are currently the most commonly used security cost allocation evaluation methods currently. TCO is a term for concepts that consider benefit on security costs in enterprises. In other words, the overall cost of using a security system is the combined cost of software/hardware purchases, maintenance costs, employee training, and staffing. However, TCO cannot be an objective security cost optimization model because the results vary depending on considered factors even in the same environment.

Finally, Gordon and Loeb [20] proposed a security cost optimization model based on an analysis of security threat probability and vulnerability probability. However, the model proposed a security cost optimization method without considering the features of the system/service and limited security budget. In addition, the security threat probability and vulnerability probability are very difficult to calculate in practice.

Different security cost optimization methods and evaluation methods have been researched. However, there has been minimal research regarding security control based security cost optimization model using security vulnerability and security controls. Consequently, we need a security cost allocation method that minimizes security vulnerability focused on security controls within a limited budget.

3. Security Cost Optimization Model

The existing security risk management models without considering security risk evaluation have some problems like the perspective of the vulnerability evaluation and security cost allocation evaluation that is different, as mentioned in the introduction. Therefore, we propose a novel security risk management model using advanced attack graph (AAG) and security vulnerability measurement (SVM) to optimize cost for security infrastructure. The model, which consists of security risk evaluation method and security cost allocation method, is based on risk management standard [26] established at ISO/IEC as shown in Fig. 2.

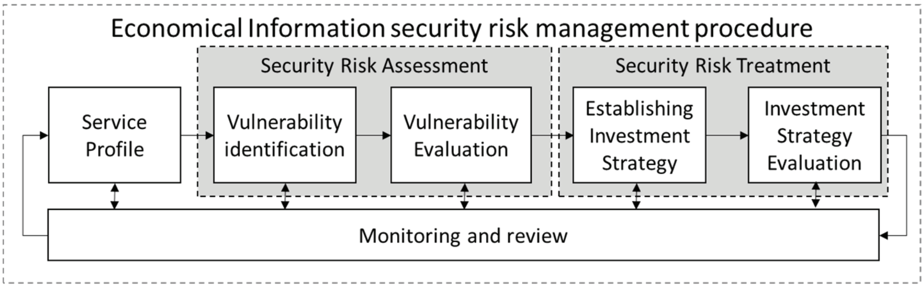

Economical Information security risk management procedure
Security Risk Assessment
Security Risk Treatment
Service Profile
Vulnerability identification
Vulnerability Evaluation
Establishing Investment Strategy
Investment Strategy Evaluation
Monitoring and review

Fig. 2. Security cost optimization model.

The procedure of security cost optimization model (Fig. 3) is performed in the following steps.

(1) **Service profile:** identify factors that service environments and security statements such as service type, security controls, etc.
(2) **Vulnerability identification:** identify security attack type and composition, such as security threat, vulnerability, etc.
(3) **Vulnerability evaluation:** draw the AAG and estimate quantitative security risk using security vulnerabilities defined in the previous phase.
(4) **Establishing cost allocation strategy:** establish optimal security cost allocation strategy considering security weight and constrained budget.
(5) **Cost allocation strategy evaluation:** evaluate the security cost allocation strategy through comparing vulnerabilities before/after allocation.
(6) **Monitoring and review:** monitor and analyze all steps of the security risk management procedure.

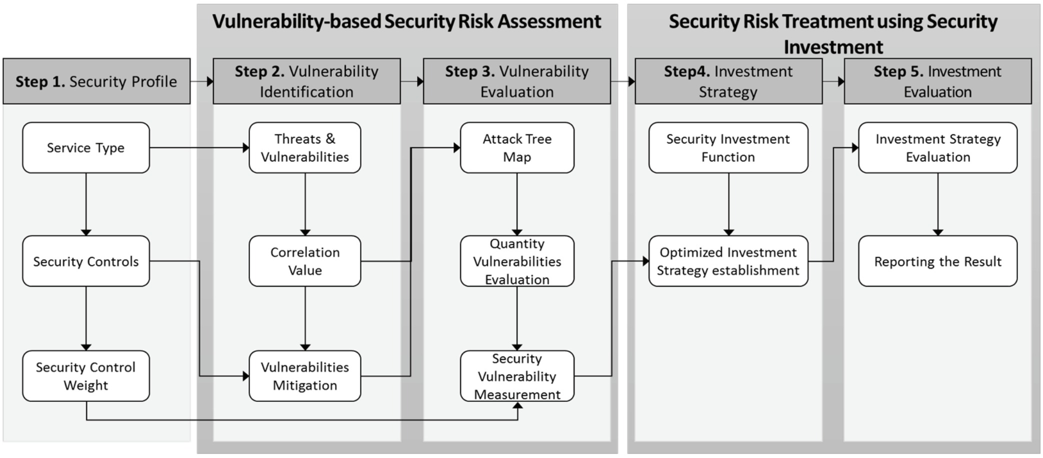

Vulnerability-based Security Risk Assessment
Security Risk Treatment using Security Investment
Step 1. Security Profile
Step 2. Vulnerability Identification
Step 3. Vulnerability Evaluation
Step4. Investment Strategy
Step 5. Investment Evaluation
Service Type
Security Controls
Security Control Weight
Threats & Vulnerabilities
Correlation Value
Vulnerabilities Mitigation
Attack Tree Map
Quantity Vulnerabilities Evaluation
Security Vulnerability Measurement
Security Investment Function
Optimized Investment Strategy establishment
Investment Strategy Evaluation
Reporting the Result

Fig. 3. Procedure of security cost optimization model.

In this paper, we will focus on detailed procedures of the security risk assessment and information security cost allocation, excluding monitoring and reviewing of the sixth phase. Moreover, this economical information security risk management model adopts the following assumptions:

- One security threat (V_1) consists of several security vulnerabilities ($V_{11}, V_{12}, V_{13} \dots$).
- The security controls are independent of each other in the investment of security controls. If we invest the security control, SC_1, it does not affect the vulnerability of other security controls ($SC_2, SC_3, \dots$).
- One of the security vulnerabilities has to match one of the security controls. Moreover, one of the security controls has more than one vulnerability.
- The currency used in the example is irrelevant; thus, we consider the values as plain numbers.

In Table 2, we summarize all the notations used in this paper.

Process of economical information security risk management

We propose a new security risk management model that considers the features of a service and a limited security budget. The proposed model follows five steps, and the following sections will provide a detailed description of each step.

Table 2. Notations

Notation	Description
V_{xy}	The y-th vulnerability in x-th threat $\mathrm{V} = \{V_{xy} \mid x = 1, \ldots, n, y =: 1, \ldots, m\}$
SC_i	The i-th security control $\mathrm{SC} = \{SC_i \mid i = 1, \ldots, k\}$
CV_{ab-cd}	The correlation value between V_{ab}(parent node) and V_{cd} (child node)
vV_{ab}^0	The initial vulnerability value of vulnerability $\mathrm{V_{ab}}$
vV_{ab}	The vulnerability value of vulnerability $\mathrm{V_{ab}}$ after AAG formula
$vV(SC_i)$	Total vulnerability value of the security control SC_i
W_i	Weight of SC_i, where $\sum W_i = 10$ and $W_i \geq 0$
z_i	The allocated cost for security control SC_i $\mathrm{Z} = \sum \{z_i \mid i = 1, \ldots, k\}$
SVM_i	The SVM of the security control SC_i $SVM = \sum \{SVM_i \mid i = 1, \ldots, k\}$
vV_{child}	The total vulnerability value of child nodes of vulnerability
F_{child}	The total vulnerability value of child nodes of vulnerability after investment
$\mathrm{F}(SC_i)$	The total vulnerability value of the security control SC_i after investment
$F_{xy}(z_i)$	The vulnerability value after investing investment cost z_i in vulnerability xy
$F_{eff}(Z)$	The efficiency of security investment
$F_{red}(Z)$	The reduction ratio of vulnerability
$F_{imp}(Z)$	The improvement ratio of security

3.1 Step 1. Define the Service Environment Parameters

This chapter identifies service types and environments, defines security control, and defines the weight of security control for each service type.

Service type

At first, we define the type of service that will define security controls and their weights. This definition of service type can be categorized into ICT parts (e.g., healthcare, internet of things, artificial intelligence, etc.) or can be categorized by service objectives (e.g., storage service, web application service, web desktop service, etc.). We might define service types on a variety of criteria.

Security controls

The security controls mean that the service provider is composed of classification of security functions or technologies. The i-th security controls (SC_i) is part of the security technology such as storage, process, network, access control, and audit [27] of the corresponding service provider. Moreover, a vulnerability has to match one or more security controls, and the security cost allocation method allocates only in security controls.

Moreover, the investment cost ($Cost_i$) in security control i includes several costs [24]: (1) implementation cost ($Cost_{imp_i}$), (2) installation cost ($Cost_{inst_i}$), (3) maintenance cost ($Cost_{main_i}$), and (4) training cost ($Cost_{train_i}$).

$$Cost_i = \ Cost_{imp_i} + Cost_{inst_i} + Cost_{main_i} + Cost_{train_i}$$

Weights of security controls

The security controls have different security control weights depending on characteristics of the service type. For example, it is important that there is availability of the service, access control, and personal identification information for a web service. However, in a storage service, it is important to have data encryption, data backup, and privilege management.

Consequently, the weight of the security control is relatively important depending on characteristics of the service type.

In 2014, to determine the weights of the security control, Na et al. [19] proposed a method to calculate the weight of the security control depending on the service type based on an AHP hierarchy model. The weight decision approach of the security control includes several decision-making methods such as an AHP model and the Delphi technique.

3.2 Step 2. Identification of Security Vulnerabilities

In this step, we identify the potential security threats and vulnerabilities that can occur in the corresponding service or system, calculate the correlation values (CVs) through correlation analysis between vulnerabilities, and define the mitigation rate according to security investments. These identified vulnerabilities and related variables are used for drawing the AAG and evaluating vulnerability (in the next step).

Threats and vulnerabilities

Most security attacks involve several sub-processes in order to achieve an attack goal. However, in a service provider aspect. However we have analyzed and defined the sub-processes of attacking vulnerabilities that are executed in order from one security threat. Therefore, we identify and respond to all of the potential security attacks on the service provider and define vulnerabilities and threats against attack sub-processes. The security threats consist of multiple vulnerabilities of a threat that operate in a regular sequence.

Correlation value between parent and child vulnerability

Since the sub-processes of attack techniques proceed in order, the vulnerabilities of parent and child in one security threat affect each other. For example, if the first attack sub-process is successful, the second attack sub-process is easier to execute. Therefore, in the security risk assessment, the correlation between attack nodes should be considered. For accurate security threat assessment, CVs are important and have a lot of influence. However, this paper does not research the derivation of correlation values. For accurate security threat assessment, CVs are important and have a lot of influence. However, in this paper, the description of derivation of CVs is omitted because it proposes an accurate security evaluation method using AAG.

Security vulnerability mitigation ratio

Security vulnerability mitigation (SVM) rate refers to the rate at which security vulnerabilities are mitigated when companies or organizations invest their security budgets. This ratio is different for each security control and also depends on the service environment or service type. In general, this ratio can also be estimated from security-enhancing data (historic or static data) from security budget investments at the company or organization.

3.3 Step 3. Evaluation of Security Vulnerabilities

To evaluate accurate security risk assessment and select an effective security cost allocation strategy, this step is the most important step to determine the investment cost for each security control in the proposed scheme. This step consists of three processes: (1) draw the AAG, (2) evaluate the values of the vulnerabilities, and (3) calculate the SVM. In addition, we describe the AAG, which has shown the overall flow of security attack using security controls, security vulnerabilities, and threats. In addition, we describe estimation of the vulnerability value and how to process the vulnerability measurement.

In exploring the security cost optimization model, this paper will be limited to proposing an AAG design, establishing an optimal security cost allocation strategy, and discussing how to evaluate the cost allocation strategy. The quantitative security risk assessment methods [28-31] and security control weight decision methods [19] are beyond the scope of the present paper. Therefore, we will just use existing quantitative security risk assessment methods and security control weight decision methods, which we do not propose.

Design the advanced attack graph

The AAG shows all known-attacks and sub-process that can occur on the system, and it helps to understand the solution for vulnerability duplicating problem. This AAG is designed for attack techniques and security controls as a countermeasure to the attack techniques.

Repetition removal vulnerability

As mentioned above, each security attack has a different goal and attack process. However, some sub-processes are common to most attack techniques. Therefore, in service risk evaluation, a common sub-process from most attacks can be duplicated, resulting in incorrect assessment results. For example, data breach and data loss are different security threats. However, both threats have the same security vulnerability such as hijacking administrator accounts. Thus, existing security evaluation methods have the problem of repeatedly evaluating the same security vulnerability based on different security threat. The important thing in this section is that the duplicated vulnerabilities are not included in the security risk assessment and security investment function. To solve this duplicated evaluation, we need to remove the duplicate vulnerability. The removal of a duplicate vulnerability in an AAG is shown in Fig. 4.

Match security controls with vulnerabilities

After eliminating the duplicate vulnerability, we classify and match the vulnerabilities with relevant security controls. Moreover, through this process, it is possible to know the security weakness point because it can know the security weakness that is not matched with the security control.

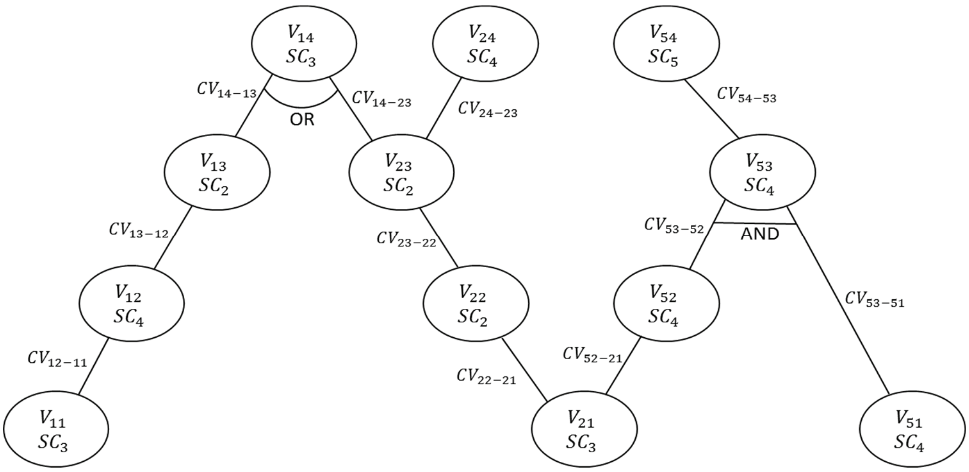
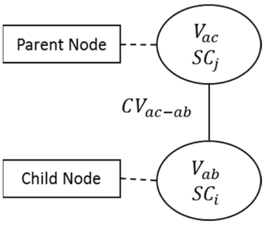
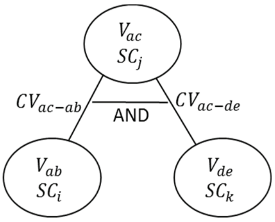
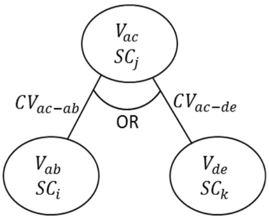


Fig. 4. Example of an AAG structure.

Draw the AAG

The AAG is composed of Normal, AND, and OR structure (Table 3). This graph can be designed as shown in Fig. 5 using three structures, based on the associated security controls matched to the interrelationships of the vulnerabilities. In addition, each vulnerability node is a parent-child relationship because the attack process proceeds sequentially. In the OR structure, if more than one child node exists, the parent vulnerability is threatened if only one child node succeeds. In the AND structure, the parent node is threatened only if all the child nodes succeed in the attack.

Table 3. Types of AAG structure

Normal structure	AND structure	OR structure
 Parent Node V_{ac} SC_j CV_{ac-ab} Child Node V_{ab} SC_i	 V_{ac} SC_j CV_{ac-ab} AND CV_{ac-de} V_{ab} SC_i V_{de} SC_k	 V_{ac} SC_j CV_{ac-ab} OR CV_{ac-de} V_{ab} SC_i V_{de} SC_k

Because a security attack is conducted in several steps sequentially, the child node affects the parent node. In this paper, the influence between the child and parent nodes is defined as the CV. Therefore, we can calculate vulnerability values (vV_{ac}) of vulnerability nodes in an AAG including the CV based on initial vulnerability values (vV_{ac}^0), as in (1)–(3).

$$\textit{Normal structure:}\ \ vV_{ac} = vV_{ac}^0 + (vV_{child} * CV) \tag{1}$$

$$\textit{OR structure:}\ \ vV_{ac} = vV_{ac}^0 + \sum(vV_{childn} * CV) \tag{2}$$

$$\textit{AND structure:}\ \ vV_{ac} = vV_{ac}^0 + \frac{\sum(vV_{childn} * CV)}{Number\ of\ V_{child}} \tag{3}$$

In a normal structure, the vulnerability node (V_{ac}) is affected the CV of a single child node, while the OR structure affects the CV of all child nodes. The AND structure is also affected also average CV of child nodes.

This AAG is designed based on attack techniques and sub-processes against the CSP; it helps to elucidate the security status based on security threats, vulnerabilities, and related security controls.

Evaluation of quantitative vulnerability

In AAG, duplicate vulnerabilities are eliminated, and vulnerabilities quantitatively assessing the number of vulnerabilities in this paragraph. In order to calculate the vulnerability value, the quantitative security risk assessment method was used. Many previous studies [28-31] have attempted to calculate vulnerability value. In this paper, the vulnerability value are calculated using the existing studies.

Security vulnerability measurement

The SVM is a criterion of the security vulnerability evaluation that considers the weight of the security control and the vulnerability value. We should consider the weight of the security control in the SVM because it has different impacts according to service type. To calculate the SVM, we need to perform first three processes: (i) design the AAG, (ii) define the weight of security controls, and (iii) calculate the vulnerability values.

In this section, we calculate the total vulnerability value of each security control and the SVM of a security control depending on the corresponding weight of that security control. Consequently, the SVM shows a vulnerability scale for each security control based on the weight of the security controls. We can analyze the security enhancement benefit using the SVM.

We classify the vulnerability value according to the security control because we will allocate in security controls. Therefore, $vV(SC_i)$ is the sum of the vulnerability values in related security control i, as shown in (4). In addition, in (5), SVM_i is determined by the multiplication of $vV(SC_i)$ and W_i and the weight of security control i. The SVM of a security service is the total SVM_i of all security controls, as follows in (5). Therefore, we can verify the security status of the corresponding security service through the SVM by considering the weight of the security control.

$$vV(SC_i) = \sum_{x=1}^{n} \sum_{y=1}^{m} vV_{xy}\ , where\ vV_{xy} \in SC_i \tag{4}$$

$$SVM_i = vV(SC_i) * W_i \tag{5}$$

$$SVM = \sum_{i=1}^{k} SVM_i \tag{6}$$

3.4 Step 4. Establish Optimal Security Cost Allocation Strategy

In this step, we establish a security investment strategy that invests in each security control based on the weights of the security controls for the minimum SVM.

Security cost allocation function

If security budgets are allocated for security controls, the related vulnerabilities will be mitigated. In addition, the vulnerability value of the vulnerability nodes will also be reduced, and the vulnerability nodes may have CV in the parent-child relationship, and thus the vulnerability value may vary depending on which security control budget is allocated.

Therefore, we define cost allocation functions of this security enhancement process for vulnerability mitigation using three parameters: (i) an initial vulnerability value, vV_{xy}^0, of a vulnerability node V_{xy}, (ii) vulnerability mitigation ratio $M\left(z_i, vV_{xy}^0\right)$ of related security control SC_i, and (iii) the affected vulnerability value of child node $CV * F_{child}$. The functions of the security vulnerability in each structure of the AAG are as follows:

$$Normal : F_{xy}(z_i) = vV_{xy}^0 * M\left(z_i, vV_{xy}^0\right) + F_{child} * CV \tag{7}$$

$$OR : F_{xy}(z_i) = vV_{xy}^0 * M\left(z_i, vV_{xy}^0\right) + \sum(F_{child} * CV) \tag{8}$$

$$AND : F_{xy}(z_i) = vV_{xy}^0 * M\left(z_i, vV_{xy}^0\right) + \overline{F_{child} * CV} \tag{9}$$

We should classify the vulnerability value after an investment in a security control to evaluate the vulnerability of each security control. The total vulnerability value after investing in security control i, denoted as $F(SC_i)$, is the sum of the vulnerability values of the vulnerability node associated with security control i. SVM is measured after allocating budget to security controls by considering the weight of each security control. Additionally, the sum of the SVMs of all security controls is the total SVM of the service. Therefore, based on total SVM of the corresponding service, we can analyze a security vulnerability and investment assessment.

Establish a security investment strategy

In this paragraph, we can calculate $F_{all}(z_i)$ and SVM_i for each security control according to the security cost allocation function. Using the various parameters described above, we can formulate an optimal security investment strategy based on optimization theory (such as the *Lagrange multiplier method*) in a limited budget.

To establish an optimal security investment strategy, it is necessary to define a security cost allocation function that can minimize the SVM using the *Lagrange multiplier* method in a limited security budget Z as follows:

$$\begin{gathered} Minimum\ SVM = \sum_{i=1}^{k}\sum_{y=1}^{m}\sum_{x=1}^{n}\left(F_{xy}(z_i) * W_i\right) \\ Subject\ to\ \sum_{i=1}^{k} z_i = Z, where\ \{z_i | z = 1, \dots, k\} \geq 0 \end{gathered} \tag{10}$$

As in the above formula, we can estimate the investment in each security control to be the minimum SVM through the *Lagrange multipli*er method. Moreover, we can also compare and evaluate different security investment strategies based on SVM.

3.5 Step 5. Evaluation of Security Cost Allocation Strategy

In this section, we analyze several security cost allocation strategies from a variety of perspectives: (i) total SVM after cost allocation, (ii) efficiency of security cost allocation, (iii) percentage of vulnerability decrease, and (iv) percentage of security improvement.

The functions used to analyze the cost allocation method from various perspectives are as follows:

This function is the sum of the vulnerability value considering the weight of the security control for all vulnerabilities. We will compare the amount of SVM change after cost allocation.

$$SVM = \begin{cases} \sum_{i=1}^{k}\sum_{y=1}^{m}\sum_{x=1}^{n}(vV_{xy} * W_i) \\ \sum_{i=1}^{k}\sum_{y=1}^{m}\sum_{x=1}^{n}F_{xy}(z_i * W_i) \end{cases} \tag{11}$$

To analyze the cost allocation effect rate of the cost, we define effect function $F_{eff}(Z)$ as (12). $F_{eff}(Z)$ is the effect rate, which is the amount of SVM change divided by total cost Z.

$$F_{eff}(Z) = \frac{\sum_{i=1}^{k}\sum_{x=1}^{m}\sum_{y=1}^{n}\left\{\left(vV_{xy} - F_{xy}(z_i)\right) * W_i\right\}}{Z} \tag{12}$$

We can calculate the percentage of vulnerability decrease, which is the amount of SVM change divided by the SVM, as follows:

$$F_{red}(Z) = \frac{\sum_{i=1}^{k}\sum_{x=1}^{m}\sum_{y=1}^{n}\left\{\left(vV_{xy} - F_{xy}(z_i)\right) * W_i\right\}}{\sum_{i=1}^{k}\sum_{y=1}^{m}\sum_{x=1}^{n}(vV_{xy}) * W_i} * 100 \tag{13}$$

To verify the percentage of security enhancement, we define function $F_{imp}(Z)$ as (14).

$$F_{imp}(Z) = \frac{\sum_{i=1}^{k}\sum_{y=1}^{m}\sum_{x=1}^{n}\{(vV_{xy}) * W_i\}}{\sum_{i=1}^{k}\sum_{y=1}^{m}\sum_{x=1}^{n}F_{xy}(z_i) * W_i} * 100 \tag{14}$$

4. Simulation of Proposed Model

In connection with our proposed model and methods, we confirm the efficiency of security cost optimization model in this chapter. Therefore, we discuss vulnerability analysis and cost allocation in security controls and evaluate cost allocation methods based on three cost allocation strategies including our proposed model.

4.1 Step 1. Security Profile

Identification of Service Type

In order to define the service type, we select a personalized webtop service [19]. The webtop service provides a highly personalized setting of an individual desktop based on web-application. We access the virtual desktop of a personal computer, such as contacts, e-mail, and files, on a personalized and familiar desktop with synchronization tools.

Definition of security controls

In this paragraph, we define security controls through a security analysis of the webtop service. For this simulation, we define security controls according to [27].

The security controls in [27] are as follows:

- SC1: Storage (S)
- SC2: Process (P)
- SC3: Network (N)
- SC4: Access Control (AC)
- SC5: Audit (AU)

Definition of Security control weight

To calculate the SVM in a webtop service, we first define the weights of the security controls.

In this paper, we define five security controls (Storage, Processing, Network, Access Control, and Audit) according to the ANP method of [19]. Therefore, we define the weights of the security controls for the webtop service as shown in Table 4.

Table 4. Weights of security controls in webtop

Security control	S	P	N	AC	AU	Total
Weight	0.58	2.14	4.17	2.04	1.07	10

4.2 Step 2. Vulnerability Identification

Identification of threats and vulnerabilities

Among the critical security threats, we select and define five threats and an attack technique for each. Moreover, we define the vulnerabilities of each attack sub-process as shown in Fig. 5.

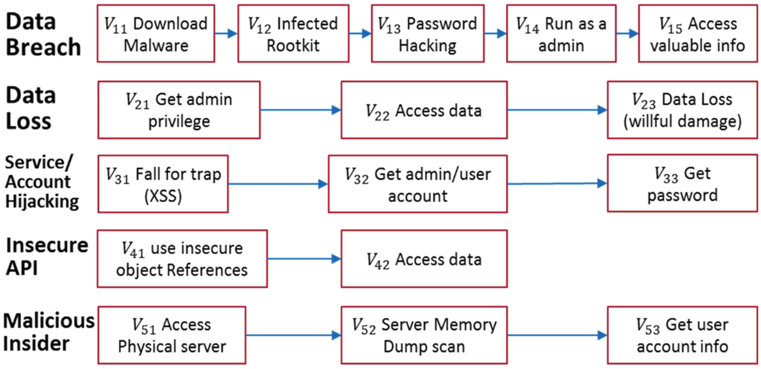

Data Breach
V_{11} Download Malware
V_{12} Infected Rootkit
V_{13} Password Hacking
V_{14} Run as a admin
V_{15} Access valuable info
Data Loss
V_{21} Get admin privilege
V_{22} Access data
V_{23} Data Loss (willful damage)
Service/ Account Hijacking
V_{31} Fall for trap (XSS)
V_{32} Get admin/user account
V_{33} Get password
Insecure API
V_{41} use insecure object References
V_{42} Access data
Malicious Insider
V_{51} Access Physical server
V_{52} Server Memory Dump scan
V_{53} Get user account info

Fig. 5. Major security threats.

- Data Breach: APT attack process to Google datacenter [16]
  $V_1 = \{V_{11}, V_{12}, V_{13}, V_{14}, V_{15}\}$
- Data Loss : Willful data damage
  $V_2 = \{V_{21}, V_{22}, V_{23}\}$
- Service/Account Hijacking: XSS attack [32]

$V_3 = \{V_{31}, V_{32}, V_{33}\}$

- Insecure API: Insecure direct object references
  $V_4 = \{V_{41}, V_{42}\}$
- Malicious Insider: Memory dump scanning [33]
  $V_5 = \{V_{51}, V_{52}, V_{53}\}$

Definition of correlation value

The CV is a value that affects the vulnerability value between child and parent node. In this simulation, however, all CVs are defined as 0.1 to simplify the evaluation process.

Definition of security vulnerability mitigation ratio

It is important to define appropriate vulnerability mitigation functions and values to establish an optimal security investment strategy.

The mitigation function for the ratio of security vulnerability mitigation was defined based on the probability of security breaches in existing security improvement models of [28,30,34,35].

The mitigation function for the security vulnerability mitigation ratio $M(z_i, v_{xy})$ is as follows:

$$M(z_i, v_{xy}) = \frac{v_{xy}}{(\alpha z_i + 1)^{\beta}}, where\ \alpha, \beta \geq 0$$

We can calculate parameters α and β of the security vulnerability mitigation function from the statistical or historical data of the security cost allocation. For example, if 36 vulnerability values change when there are 100 cost with 100 vulnerability values, we determine that parameters α and β are 0.079 and 0.468, respectively. In this example, we define the vulnerability mitigation ratio based on historical data.

In this section, we define the values of variables α and β as shown in Table 5 and Fig. 6.

Table 5. Values of variables α and β

SC_i	SC_1	SC_2	SC_3	SC_4	SC_5
α	0.078	0.073	0.077	0.047	0.068
β	0.103	0.123	0.162	0.236	0.249

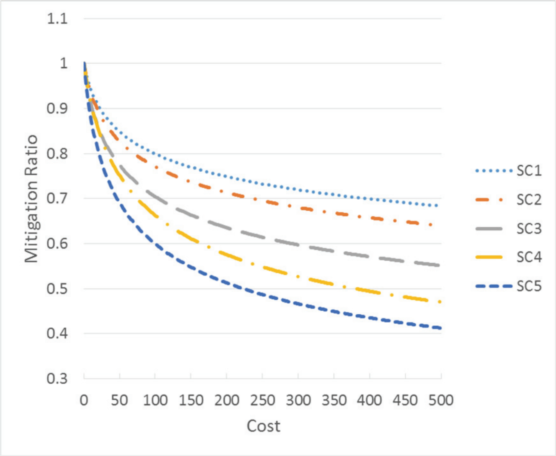


Fig. 6. Mitigation ratio of security vulnerability.

4.3 Step 3. Vulnerability Evaluation

Design of AAG for webtop services

To design an AAG, two processes need to be performed first. The first is to eliminate duplicate vulnerabilities, and the second is to match each vulnerability with a security control.

Through the security profile of the webtop service, we detected duplicate vulnerabilities by obtaining the password (V_{13}, $V_{33,}$ $V_{21,}$ and V_{53}) and accessing the data (V_{15}, $V_{22,}$ and V_{42}). We then eliminate duplicate vulnerabilities and match the vulnerability with the related security control.

After two processes, the following AAG is drawn as shown in Fig. 7.

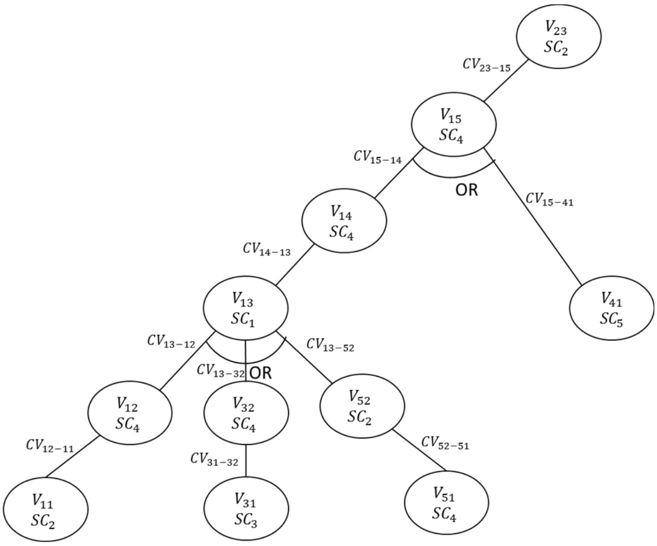


Fig. 7. Designed AAG of security simulation.

Evaluation of quantitative vulnerabilities

The vulnerability nodes de-duplicated through AAG are assessed and define initial vulnerability value based on the existing quantitative security assessment methods [28-31], as shown in Table 6.

Table 6. Attack-node configurations

Vulnerability	Parent node	Child node	$\boldsymbol{vV^0}$	Related SC
$\boldsymbol{V_{11}}$	V_{12}	-	45	SC2
$\boldsymbol{V_{12}}$	V_{13}	V_{11}	21	SC4
$\boldsymbol{V_{13}}$	V_{14}	V_{12}, V_{32}, V_{52}	56	SC1
$\boldsymbol{V_{14}}$	V_{15}	V_{13}	17	SC4
$\boldsymbol{V_{15}}$	V_{23}	V_{14}, V_{41}	13	SC4
$\boldsymbol{V_{23}}$	-	V_{15}	15	SC2
$\boldsymbol{V_{31}}$	V_{32}	-	57	SC3
$\boldsymbol{V_{32}}$	V_{13}	V_{31}	21	SC4
$\boldsymbol{V_{41}}$	V_{15}	-	63	SC5
$\boldsymbol{V_{51}}$	V_{52}	-	24	SC2
$\boldsymbol{V_{52}}$	V_{13}	V_{51}	21	SC4
Total			353	

The vulnerability values are calculated by considering the initial vulnerability value and the CV of the corresponding vulnerability node. In addition, it classifies vulnerability nodes according to each security control and calculates the total vulnerability value in each security control based on Table 6, as shown in Table 7.

Table 7. Summary of security controls

Security control	Correlated vulnerabilities	Sum of vV^0	Sum of vV
SC1	V_{13}	56	63.56
SC2	V_{11}, V_{23}, V_{52}	81	85.564
SC3	V_{31}	57	57
SC4	$V_{12}, V_{32}, V_{51}, V_{14}, V_{15}$	96	121.192
SC5	V_{41}	63	63
Total		353	390.316

Security vulnerability measurement

The SVM is calculated as a vulnerability value of each vulnerability and the weight of the security control using (2)-(4) as Tables 8 and 9.

Table 8. Vulnerability values of attack nodes after security cost allocation

Vulnerabilities	Vulnerability values (vV)	SVM	Security controls
V_{11}	45	96.3	SC2
V_{12}	25.5	52.02	SC4
V_{13}	63.56	36.865	SC1
V_{14}	23.356	47.646	SC4
V_{15}	21.636	44.137	SC4
V_{23}	17.164	36.73	SC2
V_{31}	57	237.69	SC3
V_{32}	26.7	54.468	SC4
V_{41}	63	67.41	SC5
V_{51}	24	48.96	SC4
V_{52}	23.4	50.076	SC2
Total	390.316	772.302	

Table 9. Security control vulnerability measurement

Security controls	Vulnerabilities	SVM
SC1	V_{13}	36.865
SC2	V_{11}, V_{23}, V_{52}	183.106
SC3	V_{31}	237.69
SC4	$V_{12}, V_{32}, V_{51}, V_{14}, V_{15}$	247.231
SC5	V_{41}	67.41
Total		772.302

4.4 Step 4. Investment Strategy

In this section, we obtain optimal security cost allocation strategy using SVM and the security cost allocation function.

The security cost allocation function is as follow:

$$\text{Minimum SVM} = \sum_{i=1}^{5}\sum_{y=1}^{4}\sum_{x=1}^{5}\left(F_{xy}(z_i) * W_i\right)$$

$$\text{Subject to} \sum_{i=1}^{5} z_i = z_1 + z_2 + z_3 + z_4 + z_5 = 500$$

We can obtain the optimal cost allocation of security controls based on *Lagrange multiplier* method as shown in Table 10 and Fig. 8.

Table 10. Costs allocation of each security control

	SC_1	SC_2	SC_3	SC_4	SC_5	**Total**
Investment cost	8.832	102.428	159.943	167.366	61.432	500

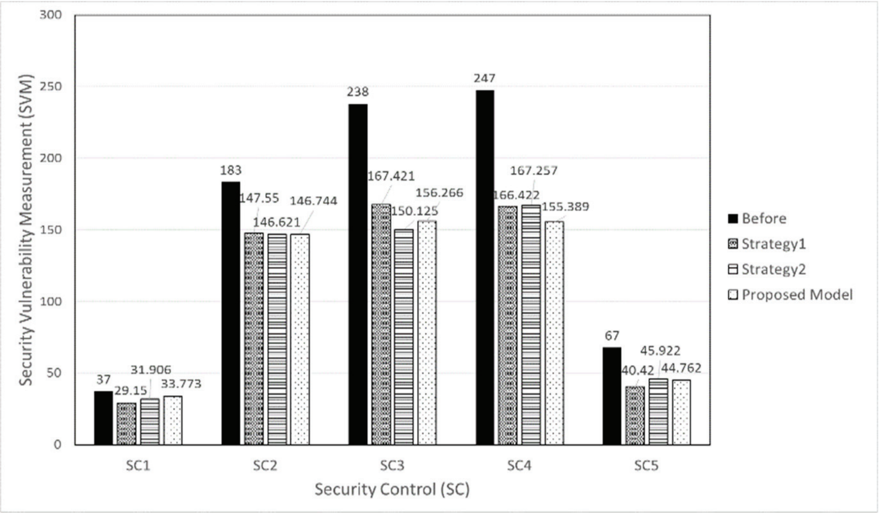


Fig. 8. Security vulnerability measurement after 500 security cost.

4.5 Step 5. Cost Allocation Strategy Evaluation

In the previous sections, we addressed the security enhancement model in order to minimize the SVM for a limited security budget in the computing environment.

In this section, we will simulate the security cost allocation strategies with a selected service [7], a webtop service with a limited security budget using previously defined parameters (vulnerability, Security Controls, SVM, etc.).

The following assumptions are made for the factors of the environment for the cost allocation evaluation:

The three scenarios are as follows.

- **Strategy 1. Equality cost allocation:** This equality cost allocation method allocates the same cost for each security control.
- **Strategy 2. Cost allocation according to weight of the security control:** This method determines the cost based on the weight of the security control according to service type. The

cost allocation rate is the same as the rate of security control weight.

- **Strategy 3. Our proposed model:** We determine the cost allocation for each security control using our scheme for the minimum SVM.

We identify the most efficient cost allocation method through simulation with three scenarios.

Evaluation security cost allocation strategies

We assign security cost allocation strategies to the three strategies mentioned above. The proposed model determines the appropriate security cost allocation for each security control by using the *language multiplier* method, which is an optimization method for efficient security cost allocation as Table 11.

The results for SVM, which is the vulnerability value after cost allocation, are shown in Table 12 for each security cost allocation strategy. In addition, the SVM change amount $-SVM$ is used to calculate $F_{eff}(Z)$, $F_{red}(Z)$, and $F_{imp}(Z)$.

Table 11. Costs of each cost allocation strategy

	Storage	Process	Network	Access control	Audit	Total
Strategy 1	100	100	100	100	100	500
Strategy 2	29	107	208.5	101.5	54	500
Our model	8.832	102.428	159.943	167.366	61.432	500

Table 12. Result of security cost allocation strategies

	Strategy1	Strategy2	Our model
SVM	772.3	772.3	772.3
iSVM	550.96	541.83	536.93
$F_{eff}(Z)$	0.4427	0.4609	0.4707
$F_{red}(Z)$ (%)	28.6595	29.8419	30.4760
$F_{imp}(Z)$ (%)	140.1728	142.5352	143.8352

As can be seen in Table 10 and Fig. 8, with a limited security budget (500) in a webtop service, we certify that an SVM of 536.93 for our proposal model is a more effective cost allocation strategy than an SVM of 550.96 for the equality cost allocation strategy and an SVM of 541.83 for the weight-oriented cost allocation strategy.

We compare strategy1 with our model and Strategy2 with proposed model to understand the results of the cost allocation, as shown in Table 13. The SVM of our model is 14.03 and 4.9 less than strategy1 and strategy2 respectively. For the effective cost allocation with a 500 security budget, our model has a 0.028 and 0.0098 more effective cost allocation than strategy1 and strategy2, respectively. With the reduced vulnerability ratio, the proposed model shows 1.8165% and 0.6341% better reduction vulnerability ratios compared to Strategy1 and Strategy2, respectively. Finally, proposed model shows a 3.6624% and 1.3% higher security improvement ratio compared to Strategy1 and Strategy2, respectively.

This evaluation shows that proposed model that considers the weights of the security controls provides a more effective security cost allocation strategy than the equality cost allocation (Strategy1) and the cost allocation scheme according to the rate of security control weights (Strategy2).

Table 13. Comparison of security cost allocation strategies

Comparison with our model	Strategy1	Strategy2
$iSVM$	-14.03	-4.9
$F_{eff}(Z)$	0.028	0.0098
$F_{red}(Z)$ (%)	1.8165	0.6341
$F_{imp}(Z)$ (%)	3.6624	1.3

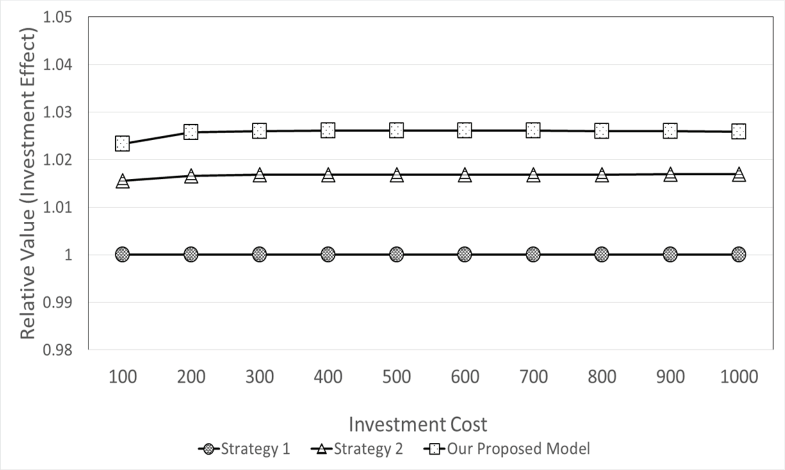


Fig. 9. Relative comparison of SVM among investment strategies.

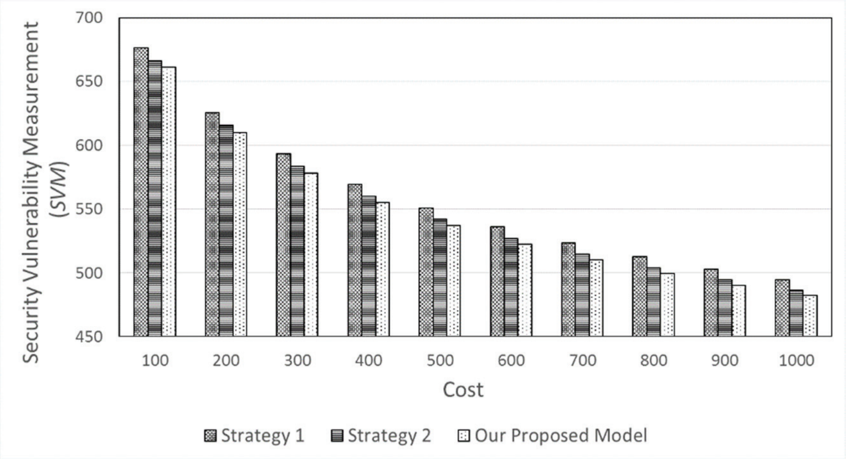


Fig. 10. Security vulnerability measurement after cost allocation.

In Fig. 9, we show SVM of each cost allocation strategies from 100 to 1000 cost. It is shown that the proposed model is the most effective cost allocation strategy when increasing cost.

Additionally, we compare the relative values of the SVM as shown in Fig. 10. When the indicator is defined by Strategy1 (average 1.0) and Strategy2 (average 1.0167), our model (average 1.02573) are the most effective. Consequentially, we verify that the proposed model is the most effective cost allocation strategy among security cost allocation strategies in a webtop service.

5. Conclusions

In this paper, instead of evaluating security risks based on security attacks and threats, we analyzed the security control composition and weight by analyzing corresponding service characteristics and service environment, and proposed an effective security enhancement scheme based on the analysis results. In addition, the problem of duplicate vulnerability evaluation of the existing security threat assessment method was solved through AAG, and limited security budget was considered.

Although this paper has covered many content security assessment methods and budget allocation methods, we can summarize them in three contributions. First, we proposed a new vulnerability evaluation method using an AAG that considers repetition removal vulnerability and CV between nodes. Second, our proposed scheme provides a security cost allocation strategy according to service type. Since each service type has a different security control weight, we consider the weight of the security control when establishing an optimal security cost allocation strategy. Finally, in the proposed scheme, the budget is limited. In fact, many companies and organizations spend a lot of budget for security enhancement, however these budgets are planned and used in a yearly budget, so the budget invested in security is limited. However, the existing security enhancement schemes do not consider this part, so the proposed method will help to plan the necessary budget for effective security enhancement.

We proposed the optimal security cost allocation method considering the service environment through the three contributions mentioned above. However, the proposed method does not describe how to define CV values. Defining CV values requires analysis and forecasting based on historical data for the service. However, the study of data analysis is beyond the scope of this paper. In future work, we will define CV values using big data analysis or machine learning based analysis methods using various environmental variables and data analysis results.

Acknowledgement

This work was supported by Institute for Information & communications Technology Planning & Evaluation (IITP) grant funded by the Korea government (MSIT) (No. 2017-0-00294, Service mobility support distributed cloud technology).

References

[1] Thales, “2017 Thales Data Threat Report: Trends in Encryption and Data Security (Global Edition),” 2017; https://www.thehaguesecuritydelta.com/media/com_hsd/report/127/document/2017-thales-data-threat-report.pdf.

[2] Barbara Filkins, “IT Security Spending Trends,” 2016; https://www.sans.org/reading-room/whitepapers/leadership/paper/36697.

[3] Ponemon Institute LLC, “2015 Global Study on IT Security Spending & Investments,” 2015; https://www.secureworks.com/resources/wp-2015-global-study-on-it-security-spending-and-investments.

[4] A. Schilling and B. Werners, “Optimizing information security investments with limited budget,” in *Operations Research Proceedings 2014*. Cham: Springer, 2016, pp. 493-499.

[5] A. Behnia, R. A. Rashid, and J. A. Chaudhry, “A survey of information security risk analysis methods,” *SmartCR*, vol. 2, no. 1, pp. 79-94, 2012.

[6] Oepn Web Application Security Project, *OWASP Top 10: The Top 10 Most Critical Web Application Security Threats: Enhanced with Text Analytics and Content by PageKicker Robot Phil 73*. North Charleston, SC: CreateSpace Independent Publishing Platform, 2014.

[7] J. Y. Park, Y. R. Shin, K. H. Kim, and E. N. Huh, "Access control framework design for personal cloud," in *Proceedings of the International Conference on Convergence Technology*, Chiang Mai, Thailand, 2013, pp. 1578-1579.

[8] W. M. Kang, S. Y. Moon, and J. H. Park, "An enhanced security framework for home appliances in smart home," *Human-centric Computing and Information Sciences*, vol. 7, article no. 6, 2017.

[9] C. D. Huang and R. S. Behara, "Economics of information security investment in the case of concurrent heterogeneous attacks with budget constraints," *International Journal of Production Economics*, vol. 141, no. 1, pp. 255-268, 2013.

[10] N. J. Brown, K. A. Jones, L. K. Nozick, and N. Xu, "Multi-layered security investment optimization using a simulation embedded within a genetic algorithm," in *Proceedings of 2015 Winter Simulation Conference (WSC)*, Huntington Beach, CA, 2015, pp. 2424-2435.

[11] H. Wang, Z. Chen, J. Zhao, X. Di, and D. Liu, "A vulnerability assessment method in industrial internet of things based on attack graph and maximum flow," *IEEE Access*, vol. 6, pp. 8599-8609, 2018.

[12] N. Gao, Y. He, and B. Ling, "Exploring attack graphs for security risk assessment: a probabilistic approach," *Wuhan University Journal of Natural Sciences*, vol. 23, no. 2, pp. 171-177, 2018.

[13] J. C. Maa, S. Chen, M. Li, and J. P. Yao, "A kind of hierarchical network vulnerability assessment model based on attack graph," in *Computer Science and Artificial Intelligence: Proceedings of the International Conference on Computer Science and Artificial Intelligence (CSAI2016)*. Singapore: World Scientific Publishing, 2017.

[14] R. Dewri, I. Ray, N. Poolsappasit, and D. Whitley, "Optimal security hardening on attack tree models of networks: a cost-benefit analysis," *International Journal of Information Security*, vol. 11, no. 3, pp. 167-188, 2012.

[15] B. Kordy and W. Wideł, "On quantitative analysis of attack–defense trees with repeated labels," in *Principles of Security and Trust*. Cham: Springer, 2018, pp. 325-346.

[16] P. Wang, W. H. Lin, P. T. Kuo, H. T. Lin, and T. C. Wang, "Threat risk analysis for cloud security based on Attack-Defense Trees," in *Proceedings of 2012 8th International Conference on Computing Technology and Information Management (NCM and ICNIT)*, Seoul, Korea, 2012, pp. 106-111.

[17] Z. Tarmudi, N. W. D. Tamsin, and J. Janteng, "A fuzzy Delphi method to rank alternatives for industry selection," *AIP Conference Proceedings*, vol. 1974, article no. 020096, 2018.

[18] Y. Tian, B. Song, and E. N. Huh, "A novel Threat Evaluation method for privacy-aware system in RFID," *International Journal of Ad Hoc and Ubiquitous Computing*, vol. 8, no. 4, pp. 230-240, 2011.

[19] S. H. Na and E. N. Huh, "A broker-based cooperative security-SLA evaluation methodology for personal cloud computing," *Security and Communication Networks*, vol. 8, no. 7, pp. 1318-1331, 2015.

[20] L. A. Gordon and M. P. Loeb, "The economics of information security investment," *ACM Transactions on Information and System Security (TISSEC)*, vol. 5, no. 4, pp. 438-457, 2002.

[21] A. Trufanov, N. Kinash, A. Tikhomirov, O. Berestneva, and A. Rossodivita, "Optimal information security investment in modern social networking," in *Complex Networks* VIII. Cham: Springer, 2017, pp. 175-182.

[22] D. Schatz and R. Bashroush, "Corporate information security investment decisions: a qualitative data analysis approach," *International Journal of Enterprise Information Systems (IJEIS)*, vol. 14, no. 2, pp. 1-20, 2018.

[23] W. Sonnenreich, J. Albanese, and B. Stout, "Return on security investment (ROSI)-a practical quantitative model," *Journal of Research and Practice in Information Technology*, vol. 38, no. 1, pp. 45-56, 2006.

[24] N. Tsalis, M. Theoharidou, and D. Gritzalis, "Return on security investment for cloud platforms," in *Proceedings of 2013 IEEE 5th International Conference on Cloud Computing Technology and Science*, Bristol, UK, 2013, pp. 132-137.

[25] A. Schilling and B. Werners, "A quantitative threat modeling approach to maximize the return on security investment in cloud computing," in *Proceedings of the 1st International Conference on Cloud Security Management (ICCSM)*, Seattle, WA, 2013, pp. 68-78.

[26] *Information technology - Security techniques - Information security risk management*, ISO/IEC 27005:2011, 2011.

[27] K. Bernsmed, M. G. Jaatun, P. H. Meland, and A. Undheim, "Security SLAs for federated cloud services," in *Proceedings of 2011 6th International Conference on Availability, Reliability and Security*, Vienna, Austria, 2011, pp. 202-209.

[28] N. Al-Safwani, Y. Fazea, and H. Ibrahim, "ISCP: in-depth model for selecting critical security controls," *Computers & Security*, vol. 77, pp. 565-577, 2018.

[29] M. S. Lund, B. Solhaug, and K. Stolen, *Model-Driven Risk Analysis: The CORAS Approach*. Heidelberg: Springer, 2010.

[30] A. Aviad, K. Wecel, and W. Abramowicz, "Semantic risk assessment for cybersecurity," in *Proceedings of International Conference on Cyber Warfare and Security*, Washington, DC, 2018, pp. 513-520.

[31] A. Sharma, V. Pal, N. Ojha, and R. Bajaj, "Risks assessment in designing phase: its impacts and issues," in *Analyzing the Role of Risk Mitigation and Monitoring in Software Development*. Hershey, PA: IGI Global, 2018, pp. 46-60.

[32] N. Chauhan, N. Singh, and B. Nagpal, "A survey on the detection of SQL injection attacks and their countermeasures," *Journal of Information Processing Systems*, vol. 13, no. 4, pp. 689-702, 2017.

[33] M. D. Nguyen, N. T. Chau, S. Jung, and S. Jung, "A demonstration of malicious insider attacks inside cloud IaaS vendor," *International Journal of Information and Education Technology*, vol. 4, no. 6, pp. 483-486, 2014.

[34] P. Wang and M. Ratchford, "Integrated methodology for information security risk assessment," in *Information Technology-New Generations*. Cham: Springer, 2018, pp. 147-150.

[35] J. Kar and M. R. Mishra, "Mitigating threats and security metrics in cloud computing," *Journal of Information Processing Systems*, vol. 12, no. 2, pp. 226-233, 2016.

Jun-Young Park **https://orcid.org/0000-0002-8481-8701**

He received his B.Eng. degree in Computer Engineering from Hannam University, Korea, in 2010, and a master's degree in Computer Engineering from the Kyung Hee University, Korea in 2012, He is currently working toward a Ph.D. degree in the Department of Computer Science and Engineering at Kyung Hee University, Korea. His research interests include cloud computing, mobile cloud computing, cloud computing security, security-as-a-service.

Eui-Nam Huh **https://orcid.org/0000-0003-0184-6975**

He earned a B.S. degree from Busan National University in Korea, a master's degree in Computer Science from the University of Texas, USA in 1995, and a Ph.D. degree from the Ohio University, USA in 2002. He is the director of Real-time Mobile Cloud Research Center. He is a chair of Cloud/BigData Special Technical Committee for Telecommunications Technology Association (TTA), and a Korean national standards body of ITUT SG13 and ISO/IEC SC38. He was also an Assistant Professor at Sahmyook University and Seoul Women's University, South Korea. He is now a Professor in the Department of Computer Science and Engineering, Kyung Hee University, South Korea. His research interests include cloud computing, screen contents coding (cloud streaming), Internet of Things, distributed real-time systems, security, and big data.