PAPER

A Quantitative Model for Evaluating the Efficiency of Proactive and Reactive Security Countermeasures

Yoon-Ho CHOI[†a)], ***Member***, **Han-You JEONG**[†b)], ***and*** **Seung-Woo SEO**[††c)], ***Nonmembers***

SUMMARY During the investment process for enhancing the level of IT security, organizations typically rely on two kinds of security countermeasures, i.e., proactive security countermeasures (PSCs) and reactive security countermeasures (RSCs). The PSCs are known to prevent security incidents *before* their occurrence, while the RSCs identify security incidents and recover the damaged hardware and software *during or after* their occurrence. Some researchers studied the effect of the integration of PSCs and RSCs, and showed that the integration can control unwanted incidents better than a single type of security countermeasure. However, the studies were made mostly in a *qualitative* manner, *not* in a *quantitative* manner. In this paper, we focus on deriving a *quantitative* model that analyzes the influence of different conditions on the efficiency of the integrated security countermeasures. Using the proposed model, we analyze for the first time how vulnerability and the potential exploits resulting from such vulnerability can affect the efficiency of the integrated security countermeasures; furthermore, we *analytically* verify that as the efficiency of PSCs increases, the burden of RSCs decreases, and vice versa. Also, we describe how to select possibly optimal configurations of the integrated security countermeasures.

key words: *evaluation of security countermeasures, proactive security countermeasures, reactive security countermeasures, complementary effects of security countermeasures, mathematical analysis*

1. Introduction

IT security breaches or violations have become one of the most important concerns in many aspects of personal, organizational and business activities. To minimize them, many organizations invest a significant amount of money to improve their security level, which represents the degree to which an organization can control the security flaws in the organization's assets such as hardware or software [1], [2]. Thus, an organization with a high security level can better protect its assets against the potential sources of harm.

Every IT asset may have vulnerabilities that can be exploited by the attacker. To achieve the highest level of protection against such vulnerabilities, most organizations employ both proactive security countermeasures (PSCs) and reactive security countermeasures (RSCs). As shown in Fig. 1, PSCs are known to identify vulnerabilities and eliminate them, and thus prevent security incidents *before* their occurrence, while RSCs detect and audit them *during or after* their occurrence. It is worth noting that since many RSCs include the solutions for protecting and recovering the damaged hardware and software *during or after* incidents, RSCs can actually reduce the likelihood of successful attack and a loss caused by a security accident and thus, the security obtained by RSCs is valuable by as much as that afforded by PSCs [3].

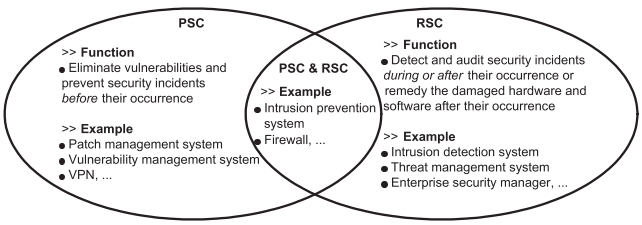

Fig. 1 Functional illustration of the security countermeasures and their examples.

As an example scenario, before security incidents occur, the Patch Management System (PMS) can take over the periodic and automatic management of software vulnerabilities that could be exploited by attackers. On the other hand, during or after their occurrence, the Intrusion Detection System (IDS) may be used to detect and audit security incidents in IT assets, and the threat management system may also be used to incorporate the system logs from different IT assets and obtain the actionable intelligence covering the complete threat lifecycle [4].

Generally speaking, vulnerabilities can be either known or unknown to the organization. Only for known vulnerabilities, PSCs can identify and eliminate them, and thus prevent them from being exploited by the attacker. That is, the unknown vulnerabilities can still be a problem because PSCs have not been adapted to tackle them. The vulnerability exploit can also be either known or unknown to the organization. For the known vulnerability exploits, RSCs can detect them while it is currently in progress. In practice, it is impossible for RSCs to cope with all of the possible vulnerability exploits, because some of the detection rules may be inaccurate. However, some of the undetected exploits can further be detected by inspecting the auditing logs of RSCs after their occurrence.

Despite the incomplete coverage of PSCs and RSCs, the above characteristics imply that there exist some interactions between their efficiency and such interactions can be used to improve the security level in a complementary man-

Manuscript received February 10, 2014.
Manuscript revised October 13, 2014.

[†]The authors are with Pusan National University, Busan, 609–735, Korea.
[††]The author is with Seoul National University, Seoul, 151–744, Korea.
a) E-mail: yhchoi@pusan.ac.kr
b) E-mail: hyjeong@pusan.ac.kr
c) E-mail: sseo@snu.ac.kr

DOI: 10.1587/transinf.2014EDP7042

Copyright © 2015 The Institute of Electronics, Information and Communication Engineers

ner. This is indeed true because after PSCs are implemented, the probability of vulnerability will decrease, which in turn reduces the burden of RSCs to detect the attacks caused by the exploits of vulnerabilities. Thus, to achieve the highest level of protection against vulnerabilities, it is necessary to analyze the interactivity of the two types of security countermeasures.

Rowe and Gallaher [5] published a conceptual study result on the optimal integration of PSCs and RSCs, which maximizes the security level subject to a fixed budget constraint (output maximization) and minimizes the security investment subject to a fixed security level (cost minimization). In their work, they assumed that a model used to evaluate the efficiency of the two types of security countermeasures is given a priori and identify an appropriate balance or combination between PSCs and RSCs in terms of a family of curves, called iso-security curves. To the best of our knowledge, however, such a quantitative model is not appropriate in practice for evaluating the interactivity between PSCs for preventing security incidents *before* their occurrence and RSCs for identifying security incidents and recovering the damaged IT asset *during or after* their occurrence, and for evaluating the efficiency of their integration. These limitations may lead to not only the inadequate deployment of the security countermeasures, but also the under- or over-investment of the budget. Thus, it is a fundamental topic to quantify the efficiency of PSCs and RSCs for achieving the cost-effective security investment as well as a high level of security.

In this paper, we propose a new model that quantifies the efficiency of PSCs and RSCs in a complementary manner and then analyze the interactivity of the two types of security countermeasures. The proposed model is based on a metric, called the 'security effectiveness (SE)', which is an information-theoretic measure of the efficiency of the security countermeasures. The metric 'SE' measures the capability to correctly distinguish the vulnerabilities as either vulnerable or invulnerable, or classify the potential exploits from such vulnerabilities as either exploit or non-exploit, when using the security countermeasures as compared to those without them. As a result of the increase of SE, the organization can reduce the damage originating from the vulnerability, or the potential exploits resulting from such vulnerability and thus improve the security level.

The main contributions of this work are as follows: (1) As a framework designed to analyze the interactivity between PSCs and RSCs, we propose for the first time a mathematical model that shows the influence of different conditions on the efficiency of the integrated security countermeasures in an analytical manner; (2) Using the proposed model, we analytically show how vulnerability and the potential exploits resulting from such vulnerability can affect the efficiency of the integrated security countermeasures in depth; (3) We also show that under various parameters of two types of security countermeasures, as the efficiency of PSCs increases, how the burden of RSCs decreases, and vice versa.

The remainder of this paper is organized as follows. In Sect. 2, we overview the relationship between SE and uncertainty, and conceptually describe how to quantify SE of security countermeasures. In Sect. 3, we present a new analytical model for quantifying SE of an integrated scenario, where SE of PSCs affects SE of RSCs. Also, in Sect. 4, we investigate the influence of the security parameters on SE of the integrated security countermeasures. Finally, we conclude this paper in Sect. 6.

2. Background

Before investigating the model to formulate SE of the security countermeasures in an information-theoretic measure, we overview the relationship between SE of the security countermeasures and uncertainty about the input information of security countermeasures, and introduce a conceptual approach that analyzes the relationship between a proactive strategy and a reactive strategy. Also, we conceptually describe how to quantify SE of each type of security countermeasures.

2.1 Relationship between SE and Uncertainty

In the case of PSCs, we assume that an IT asset is vulnerable with a probability v in the absence of PSCs. Given v, the uncertainty of the input without PSCs is equal to the sum of remaining uncertainty and the uncertainty reduction associated with the input of PSCs. Here, uncertainty represents the degree of the vulnerability of the IT asset. If PSCs can eliminate the vulnerabilities with probability 1.0, it is clear that the remaining uncertainty associated with the input of PSCs is 0. This maximum reduction of the uncertainty means that all the vulnerabilities can be eliminated with 100% confidence. However, because a practical PSC cannot remove unknown vulnerabilities, there are always some vulnerabilities after the PSC eliminates known vulnerabilities. In practice, this probability can range from 1.0 to 0.0. As the probability decreases from 1.0 to 0.0, the reduction of the uncertainty associated with the input of PSCs decreases. When the probability is 0, the reduction of the uncertainty associated with the input of PSCs is 0. Given v, this minimum reduction of the uncertainty means that PSCs do not affect the output of PSCs and thus, any vulnerabilities are not eliminated at all.

Based on these observations, we note that a reduction of the uncertainty associated with the vulnerability corresponds to an increase of SE of PSCs. Therefore, as the reduction of the uncertainty associated with the input of PSCs decreases or increases, SE of PSCs decreases or increases, respectively. The fact that the remaining uncertainty associated with the input of PSCs is higher than 0 indicates that the vulnerabilities can still be exploited by the attacker. During or after the vulnerabilities have been exploited, RSCs try to detect and audit the occurrence of the vulnerability exploit.

For RSCs, the uncertainty associated with the input without RSCs is equal to the sum of the remaining uncertainty and the reduction of the uncertainty associated with

the input of RSCs. If RSCs can detect the possible exploit with a probability of 1.0 and detect the usage of a non-vulnerability as being normal with a probability of 1.0, it is clear that the remaining uncertainty associated with the input of RSCs is 0, since all vulnerability exploits will be detected and audited using its pre-defined detection rules. However, in practice, some vulnerability exploits may not be detected and some non-vulnerability exploits may be identified as vulnerability exploits because of inaccuracies and the lack of pre-defined detection rules and thus, in reality, the remaining uncertainty is larger than 0. Specifically, when all of the known vulnerabilities are eliminated by PSCs and thus, all of the vulnerability exploits result from unknown vulnerabilities, the remaining uncertainty associated with the input of RSCs may have a smaller value. Here, the reduction of the uncertainty associated with the input of RSCs may be minimized. This minimum reduction of the uncertainty associated with the input of RSCs means that RSCs produce alerts for events without any confidence, since no accurate detection rules exist for these unknown vulnerability exploits.

To increase reduction of the uncertainty or decrease the remaining uncertainty associated with the input of RSCs, RSCs can search the auditing logs for vulnerability exploits. In this way, the reduction of the uncertainty can be increased and thus, the remaining uncertainty is decreased. That is, as the true positive ratio of RSCs increases from 0.0 to 1.0, the reduction of the uncertainty associated with the input of RSCs increases.

Based on the above observations, we note that a reduction of the uncertainty associated with the input of RSCs corresponds to an increase of their SE. Therefore, as the reduction of the uncertainty associated with the input of RSCs decreases or increases, their SE decreases or increases, respectively.

2.2 iso-security curve

Rowe and Gallaher [5] introduced the so-called iso-security curves. As shown in Fig. 2, x-axis and y-axis of each iso-security curve represent a proactive strategy and a reactive strategy, respectively, and the curves farther from the origin have higher levels of security. Also, curve #1 has the highest security level than the curves #2 and #3.

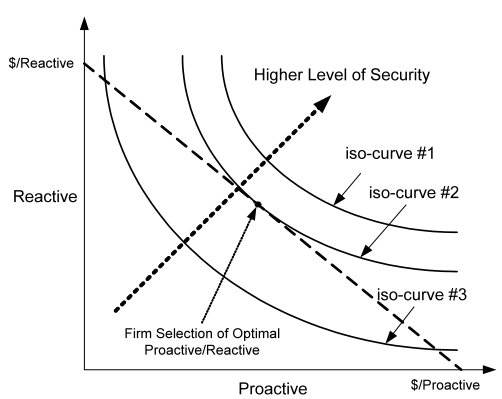

Fig. 2 iso-curves for firm selection of optimal proactive/reactive [5].

From the view points of output (the security level) maximization and cost minimization, these curves are used to find the optimal integration of the proactive strategy and the reactive strategy (firm selection of optimal proactive/reactive in Fig. 2). However, usage of these so-called iso-security curves is limited due to the followings. First, since these curves are not drawn by considering the influence of different security parameters on SE of security countermeasures, these curves show only a simple conceptual relationship between PSCs and RSCs. Second, different from general proactive and reactive strategies, SE of PSCs cannot be equal to that of RSCs. That is, the main function of PSCs is to prevent the security incidence *before* its occurrence while that of RSCs is to detect and audit it *during or after* the occurrence of the security incidence. However, these curves assume that SE of PSCs is the same as SE of RSCs.

2.3 Derivation of SE of Security Countermeasures

For better understanding, we consider PMS and IDS as representative examples of PSCs and RSCs, respectively. With PMS, we assume that the purpose of PSCs is to maximize the probability that the vulnerability is patched (identified and eliminated) before its exploit. On the other hand, with IDS, the purpose of RSCs can be expressed in twofolds: (1) to maximize the probability of an alert generation in case of a vulnerability exploit; and (2) to minimize the probability of a false alert in case of the normal behavior.

Let us first consider SE of PMS. Given vulnerabilities in an IT asset, the PMS will try to eliminate them through patching the system. For known vulnerabilities, the PMS can issue a patch, but for unknown vulnerabilities, the PMS cannot issue it. That is, the patch success rate is given as a unique decision variable for calculating the capability of the PMS. This implies that a simple probability model is sufficient to evaluate SE of PMS.

Next, let us consider SE of IDS. During or after a vulnerability is exploited, IDS may detect the vulnerability exploit. In some cases, however, IDS may not be able to detect it, which leads to a false negative. Also, even though no exploits of the vulnerability takes place, IDS may detect an event, which is known as a false positive. That is, the true detection rate and the false positive rate are given as decision variables for calculating the capability of IDS [6]. Note that different decision variables can have different improvement results [7]. For example, even though the false positive rate decreases, the true detection rate may not increase. On the other hand, even though the false positive rate increases, the true detection rate may not decrease. This implies that a simple detection probability model is not sufficient to evaluate SE of IDS. Therefore, we need to define a new security model that takes into account all of the system parameters in a unified manner.

Gu et al. [7] studied a metric that defines the capability of an IDS to classify the input events correctly. They an-

Table 1 Terms & notation.

Terms	Notation
v	Probability that IT assets are vulnerable with, where $0 \leq v \leq 1$
u	Probability that PSCs fail at eliminating vulnerabilities of IT assets with, where $0 \leq u \leq 1$
q	Probability of vulnerability exploits, where $0 \leq q \leq 1$
r	False positive ratio of RSCs, where $0 \leq r \leq 1$
s	False negative ratio of RSCs, where $0 \leq s \leq 1$
X_P	Input random variable for PSCs, $X_P \in \{0, 1\}$
Y_P	Output random variable for RSCs, $Y_P \in \{0, 1\}$
X	Input random variable for the unified security countermeasures, $X \in \{0, 1\}$
Y_1	Random variable for expressing status of the target asset after vulnerability elimination by PSCs, $Y_1 \in \{0, 1\}$
Y_2	Random variable for expressing status of the target asset after vulnerability exploit by the attacker, $Y_2 \in \{0, 1\}$
Z	Output random variable associated with the unified security countermeasures, $Z \in \{0, 1\}$
α	Ratio of SE of RSCs over SE of PSCs ($0 \leq \alpha \leq 1$)
$U_{P\|R}$	Uncertainty reduction ratio provided by PSCs, given RSCs
$U_{R\|P}$	Uncertainty reduction ratio provided by RSCs, given PSCs
U_{PR}	Uncertainty reduction ratio provided by the unified security countermeasure
I_{PR}	Monetary investment in integrated security countermeasures
E_{PR}	Expected benefits of an investment in the integrated security countermeasure
EN_{PR}	Expected net benefits of an investment in the integrated security countermeasure

alyzed the capability of IDS from an information-theoretic viewpoint [8], and proposed a new metric based on information entropy, called the Intrusion Detection Capability or CID, which is simply the ratio of the reduction of the uncertainty of an IDS input for a given IDS output. The authors note that the IDS output should faithfully reflect the "truth" about the input (whether there is an intrusion or not) and from the information-theoretic point of view, IDS should have less uncertainty about the input given its output. From the in-depth analysis, they show that CID is more sensitive to changes in different conditions than the previous evaluation metrics based on the statistical analysis [9]–[12], ROC (receiver operating characteristic) curve-based analysis [13]–[15] and cost analysis [16].

As an extension, our work is based on Gu et al.'s study in the sense that SE of the security countermeasures is defined from an information-theoretic viewpoint. However, we note that Gu et al. do not consider SE of the integrated security countermeasures, i.e., the integration of PSCs and RSCs. More specifically, the applicability of their model is only limited to RSCs, because it does not take into account the interactions between PSCs and RSCs. On the contrary, most of the organizations have a tendency to employ the integrated security countermeasures, because they can maximize their security level via complementary operation of different countermeasures [5]. To account for this trend, we need a new mathematical model that can apply to a general scenario where the two types of security countermeasures are deployed to protect the organizations.

3. Model for SE of Security Countermeasures

To analyze the interactivity of PSCs and RSCs, we propose a new analytical model, which is a mathematical model in the form of an uncertainty model based on information theory. Terms and notations in this paper are summarized at Table 1.

3.1 Abstract Model

To describe the abstract model for the integrated security countermeasures, let us consider the relationship between vulnerabilities and their exploits, with and without the security countermeasures. While PSCs are not operating, the attacker can exploit the known and unknown vulnerabilities. Otherwise, the known vulnerabilities can be eliminated and thus, those vulnerabilities cannot be exploited. For only the remaining vulnerabilities, the attacker may damage the target asset by exploiting them. Because there exists no probability of vulnerability exploits from false positives by PSCs, we consider only the probability that PSCs fail at eliminating vulnerabilities of IT assets with.

While RSCs are not operating, the vulnerability exploits resulting from the known and unknown vulnerabilities cannot be detected. On the other hand, while PSCs are not operating and RSCs are operating, the vulnerability exploits resulting from the known and unknown vulnerabilities may be detected. Also, while PSCs and RSCs are operating, the unknown vulnerability exploits may be detected. This is because some of the unknown vulnerability exploits can be detected by inspecting the auditing logs of RSCs after their occurrence.

Based on the above observation, the conceptual meaning of five key parameters, i.e., v, u, q, r, and s can be summarized as follows:

- v: Probability v is defined as the number of vulnerabilities of IT assets that can be exploited by attackers, including not only the known vulnerabilities but also the unknown vulnerabilities, to total access patterns of IT assets. Note that, if the value of parameter v is large, the IT asset is more vulnerable to security attacks.
- u: Probability u is the remaining vulnerability probability after the PSC eliminates known vulnerabilities in the IT asset. Because the IT asset has some unknown

vulnerabilities after the PSC eliminates known vulnerabilities, the attacker still has non-zero probability that they can exploit the unknown vulnerabilities. Note that, if the security administrator invests more budget to improve the performance of the PSC, the vulnerability remaining probability becomes smaller.

- q: Probability q is the probability of the vulnerability exploits by attackers. Because this probability strongly depends on the characteristics of the attackers, we assume that the probability is determined by the exterior security environments.
- r **and** s: The RSC makes its decision about the vulnerability exploit by extracting the common patterns of the attacking traffic to the IT asset. Therefore, there is always non-zero possibility that
  - The RSC misunderstand the normal traffic as the attacking traffic with the probability r, which is called the false positive rate. It is important to restrict or to minimize r because it may lead to unwanted sacrifice of the normal traffic.
  - The RSC may not detect the attacking traffic with the probability s, which is called the false negative rate. It is also important to limit s because it may harm the IT asset.

Also, we can derive the abstract models of the integrated security countermeasures as follows. For PSCs, a target asset can be denoted as a vulnerable system that is vulnerable with probability v and invulnerable with probability $1 - v$. After PSCs identify the known vulnerabilities, the target asset can be vulnerable with probability vu and invulnerable with probability $(1 - vu)$. Here, regardless of the existence of RSCs, the vulnerability status of the target asset is determined by PSCs. Thus, we can express PSCs in the form of a system model whose input indicates the system vulnerability status, i.e., invulnerable or vulnerable, and whose output indicates the vulnerability identification status, i.e., identification or non-identification. For RSCs, a target asset can be a vulnerable system whose remaining vulnerabilities with probability vu are either exploited with probability q or not exploited with probability $(1 - q)$. As RSCs classify the potential exploits from the remaining vulnerabilities as exploit or non-exploit, they can be expressed in the form of a system model whose input indicates the vulnerability exploit status, i.e., vulnerability non-exploit or vulnerability exploit, and whose output indicates the corresponding alert generation, i.e., alert or no alert.

With these insights, we represent PSCs as a binary Markovian channel model as shown in Fig. 3: The input status of PSCs represents the awareness of the vulnerabilities, either invulnerable or vulnerable. We denote it by a binary random variable X_P, where $X_P = 0$ indicates invulnerability and $X_P = 1$ indicates vulnerability. The output of PSCs indicates whether vulnerabilities are identified or not. We denote it by a binary random variable Y_P, where $Y_P = 0$ indicates an identification of the vulnerability and $Y_P = 1$ indicates non-identification of the vulnerability.

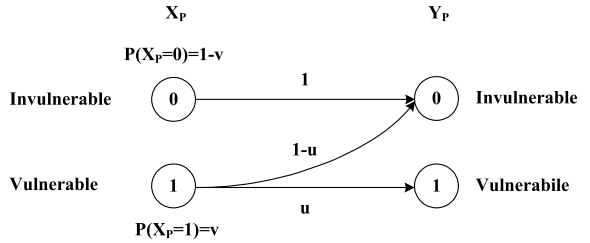

Fig. 3 A binary Markovian channel model for PSCs.

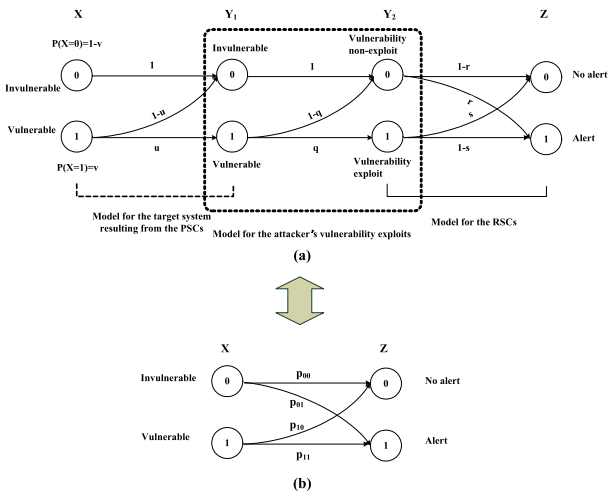

Fig. 4 Abstract models: (a) for the PSCs, the attacker's vulnerability exploit and the RSCs; and (b) for the unified security countermeasures.

We assume that the known vulnerabilities in the target asset can be identified ($Y_P = 1$) by PSCs with probability $\Pr\{Y_P = 1|X_P = 1\} = 1 - u$. On the other hand, the unknown vulnerabilities are still the problem with probability $\Pr\{Y_P = 0|X_P = 1\} = u$.

In Fig. 4 (a), we show a binary Markovian channel model for RSCs. The input of RSCs represents the status of the vulnerability exploits while PSCs are operating. That is, the input of RSCs is denoted as the output of PSCs associated with the vulnerability exploits by the attacker (: dotted box in Fig. 4 (a)). After the known vulnerabilities being eliminated, the status of the target asset is denoted as a binary random variable Y_1, where $Y_1 = 0$ indicates invulnerability from a successful vulnerability elimination and $Y_1 = 1$ indicates vulnerability from a successful vulnerability elimination. Also, after the remaining vulnerabilities being exploited, the status of the target asset is denoted as a binary random variable Y_2, where $Y_2 = 0$ indicates a vulnerability non-exploit and $Y_2 = 1$ a vulnerability exploit. The output of RSCs represents whether the corresponding alerts for vulnerability exploit and vulnerability non-exploit from the remaining vulnerabilities are correctly generated or not. We denote it by a binary random variable Z, where $Z = 1$ indicates alert generation and $Z = 0$ alert non-generation.

Based on the abstract model in Fig. 4 (a), we can derive an abstract model of the integrated security countermeasures into a binary Markovian channel model in Fig. 4 (b),

which takes into account the security parameters of PSCs and RSCs in a unified manner. Their abstract model is equivalent to the abstract model of RSCs, but has the different input from that of RSCs. The input of the integrated security countermeasures represents the awareness of the vulnerabilities, either invulnerable or vulnerable. We denote it by a binary random variable X, which is an input of PSCs. The output of the integrated security countermeasures indicates whether the corresponding alerts for vulnerability exploit and vulnerability non-exploit from such vulnerabilities are correctly generated or not. We denote it by a binary random variable Z, which equals to an output of RSCs.

Based on the equivalence between the abstract models shown in Figs. 4 (a) and 4 (b), we can compute the following transition probabilities, i.e., P($Z|X$) for $X = \{0, 1\}$ and $Z = \{0, 1\}$. The probabilities of whether the corresponding alerts for vulnerability non-exploit from the invulnerability are generated or not are computed as $P(Z = 1|X = 0) = p_{01} = r$ and $P(Z = 0|X = 0) = p_{00} = 1-r$, respectively. Similarly, the probabilities of whether the corresponding alerts for vulnerability exploit from the vulnerability are generated or not are computed as $P(Z = 1|X = 1) = p_{11} = uq(1 - s) + (1 - u)r + u(1 - q)r$ and $P(Z = 0|X = 1) = p_{10} = (1-u)(1-r)+u(1-q)(1-r)+uqs$, where $(1-u)\cdot 1\cdot(1-r)$ for a transition of $(X, Y_1, Y_2, Z) = (1, 0, 0, 0)$; $u\cdot(1-q)\cdot(1-r)$ for another transition of $(X, Y_1, Y_2, Z) = (1, 1, 0, 0)$; and $u \cdot q \cdot s$ for the other transition of $(X, Y_1, Y_2, Z) = (1, 1, 1, 0)$. Also, $P(Z = 1|X = 1) = 1 - P(Z = 0|X = 1)$.

3.2 Uncertainty Model

Based on the abstract models shown in Figs. 3 and 4, we now formulate SE of the integrated security countermeasures. To formulate this SE, we obtain the likelihood that PSCs identify vulnerabilities correctly and RSCs alert us as a vulnerability exploit. Recall that this likelihood is expressed based on the uncertainty reduction associated with the input of the security countermeasures after their output is known. For PSCs the likelihood that they identify vulnerabilities correctly can be expressed as the uncertainty reduction ratio in vulnerabilities, provided by the integrated security countermeasures, as follows:

$$U_{P|R}(v, u) = U_P(v, u), \tag{1}$$

because this uncertainty reduction ratio does not depend on SE of RSCs.

From Fig. 3, in the absence of PSCs, the entropy associated with the input random variable X_P determines the uncertainty that the system is vulnerable, $X_P = \{0, 1\}$. Here, the entropy [8] is formulated as

$$H(X_P) = -\sum_{x_p=0}^{1} p(x_p) \log p(x_p), \tag{2}$$

where $p(x_p)$ means the probability mass function of a discrete random variable X_P, i.e., $P(X_P = 0) = 1 - v$ and $P(X_P = 1) = v$. Also, the conditional entropy of the input random variable X_P given the output random variable Y_P, $Y_P = \{0, 1\}$, determines the remaining uncertainty that the system is either vulnerable after vulnerabilities are identified ($Y_P = 0$) or not ($Y_P = 1$). Here, the conditional entropy [8] is formulated as

$$H(X_P|Y_P) = -\sum_{y_p=0}^{1} p(y_p) \sum_{x_p=0}^{1} p(x_p|y_p) \log p(x_p|y_p). \tag{3}$$

Furthermore, the mutual information of the input random variable X_P and the output random variable Y_P represents the amount of reduction of uncertainty in the input random variable X_P after the output random variable Y_P becomes known. That is, this mutual information implies the amount of correct vulnerability identification by PSCs. Here, the mutual information [8] is formulated as

$$I(X_P; Y_P) = H(X_P) - H(X_P|Y_P), \tag{4}$$

where $I(X_P; Y_P) = I(Y_P; X_P) = H(Y_P) - H(Y_P|X_P)$ by symmetry. Thus, in the same way that Gu et al. [7] studied a metric that defines the capability of an IDS, the uncertainty reduction ratio of the input random variable, X_P, with PSCs as compared to the case without them can be expressed into:

$$U_P(v, u) = \frac{\mathrm{I(Y_P; X_P)}}{\mathrm{H(X_P)}}, \tag{5}$$

where $0 \le I(X_P; Y_P) = I(Y_P; X_P) < H(X_P)$, $0 \le U_P(v, u) < 1$. Here, because there exist unknown vulnerabilities, $I(Y_P; X_P) < H(X_P)$. Also, the value of $p(y_p|x_p)$ depends on u and the value of $p(x_p)$ depends on v. For RSCs the entropy of the input variable Y_2 determines the uncertainty that the remaining vulnerabilities, resulting from vulnerability elimination by PSCs, are exploited by the attacker. Also, the mutual information of the input random variable Y_2 and the output random variable Z of RSCs determines the amount of reduction of uncertainty in the input random variable Y_2 after the output random variable Z becomes known. Thus, we can derive the uncertainty reduction ratio, provided by the integrated security countermeasures, in the potential exploits from the remaining vulnerabilities as follows:

$$U_{R|P}(v, u, q, r, s) = \alpha \cdot \frac{\mathrm{I(Z; Y_2)}}{\mathrm{H(Y_2)}}, \tag{6}$$

where $0 \le I(Z; Y_2) = I(Y_2; Z) < H(Y_2)$ and $0 \le U_{R|P}(v, u, q, r, s) < 1$. Here, because there exist unknown vulnerability exploits, $I(Y_2; Z) < H(Y_2)$. The value of $p(y_2)$ depends on v, u and q, the value of $p(z|y_2)$ depends on r and s. Also, we denote α ($0 \le \alpha \le 1$) as the ratio of SE of RSCs over SE of PSCs because PSCs prevent security incidents *before* their occurrence while RSCs identify security incidents and recover the damaged IT asset *during or after* their occurrence.

For $v = 0$ or $u = 0$, the probability of the target asset being vulnerable is zero, i.e., $\mathrm{P}(Y_1 = 1) = 0$, and also, the probability of vulnerabilities being exploited is zero, i.e., $\mathrm{P}(Y_2 = 1) = 0$. Here, $\mathrm{P}(Y_1 = 1) = 0$ means that all the vulnerabilities in the target asset are eliminated and thus, SEs

of PSCs and RSCs are one, respectively. For $v \neq 0$ and $u = 1$, $P(Y_1 = 1) = v$. This means that SE of PSCs is zero and then, if $r = 0$ and $s = 0$, SE of RSCs has the maximum one. For $r = 1$ and $s = 1$, we assume that SE of RSCs is zero. Thus, the uncertainty reduction ratio provided by RSCs ranges from 0 to 1.

Also from the abstract model in Fig. 4 (b), we can finally derive the uncertainty reduction ratio provided by the unified security countermeasure, which has the capability of both PSCs and RSCs:

$$U_{PR}(v, u, q, r, s) = \frac{\mathrm{I(Z; X)}}{\mathrm{H(X)}}, \tag{7}$$

where $0 \leq U_{PR}(v, u, q, r, s) < 1$ and the value of $p(x)$ depends on v. For the proof, we note that SE of the unified security countermeasure indicates the capability to correctly identify vulnerabilities as vulnerable or invulnerable, *and* classify the potential exploits from such vulnerabilities as exploit or non-exploit. Also, we note that when we determine the uncertainty reduction ratio resulting from the unified security countermeasure, SE of each type of security countermeasures should be quantified without overlap. Thus, based on Fig. 4 (b), it is possible to denote SE of the unified security countermeasure as the uncertainty reduction ratio in vulnerabilities.

4. Influence of Security Parameters on SE

Different from the previous analysis results [7], we investigate the influence of parameters of security countermeasure and given security parameters, i.e., v, u, q, r and s, on SE of the integrated security countermeasures and the unified security countermeasure.

4.1 Influence of Given Parameters

We investigate the influence of the two uncontrollable parameters v and q, which cannot be controlled by an organization, on the security countermeasures. Under diverse vulnerability levels of an IT asset, it is shown that RSCs are effective to improve the security level of the organization as SE of PSCs decreases. Although the security achieved by RSCs is not equivalent to that of PSCs, this result implies that RSCs are the good candidates to effectively improve the security level of the organization when SE of PSCs is constrained. Also, under diverse vulnerability exploit levels, it is shown that RSCs are effective to improve the security level of the organization as the likelihood that RSCs can classify the potential exploits from the remaining vulnerabilities, given SE of PSCs, increases.

4.1.1 Influence of v

Figure 5 shows the influence of v on SEs of PSCs and RSCs, given $\alpha = 0.1$: (1) $u = 0.7$, $q = 0.3$, $r = 0.001$ and $s = 0.001$; (2) $u = 0.7$, $q = 0.3$, $r = 0.01$ and $s = 0.001$; and (3) $u = 0.7$, $q = 0.3$, $r = 0.01$ and $s = 0.01$. Here, we assume that the IT asset is vulnerable with a probability $v \in \{10E-7, 0.1\}$ because it has some smaller level of vulnerability in practice and SE needs to be sensitive in the change of such small level of vulnerability. The so-called security countermeasure operating characteristics (SCOC) curve in Fig. 5 relates SEs of PSCs and RSCs, and compares them as the value of v changes. In Fig. 5, the x-axis is SE of PSCs, calculated from Eq. (1); the y-axis is SE of RSCs, calculated from Eq. (6). For example, $U_{R|P}(0.005, 0.7, 0.3, 0.001, 0.001)$ in the y-axis can be calculated as follows: $U_{R|P}(0.005, 0.7, 0.3, 0.001, 0.001) = 0.1 \times (I(Z; Y_2)/H(Y_2))$, where $I(Z; Y_2) = H(Y_2) - H(Y_2|Z)$. Thus, $U_{R|P}(0.005, 0.7, 0.3, 0.001, 0.001) = 0.1 \times (1 - \frac{H(Y_2|Z)}{H(Y_2)}) \approx 0.094$, where $H(Y2) \approx 0.0255$ and $H(Y_2|Z) \approx 0.0015$.

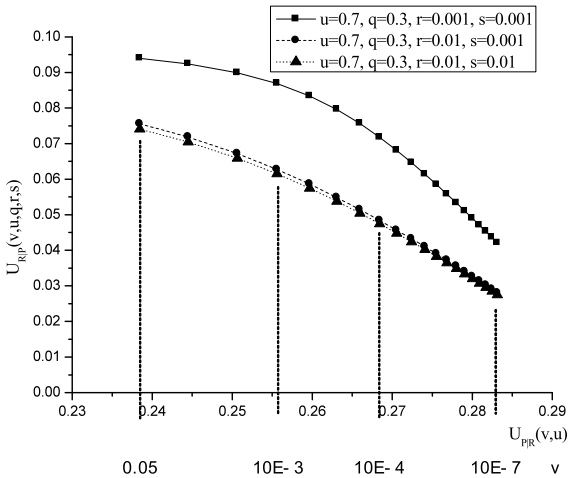

Fig. 5 Influence of v on SEs of PSCs and RSCs ($U_{P|R}(v, u)$ and $U_{R|P}(v, u, q, r, s)$), where $\alpha = 0.1$.

If the IT asset is perfectly invulnerable ($v = 0$), then SE of the integrated security countermeasures is maximized ($U_{P|R}(v, u) = 1$ and $U_{R|P}(v, u, q, r, s) = 1$). In Fig. 5, it is shown that at some sufficiently larger level of vulnerability, SE of PSCs decreases slowly as the likelihood that PSCs identifies vulnerabilities correctly decreases. On the contrary, SE of RSCs increases as SE of PSCs decreases. This is because as the probability of a target asset being vulnerable increases, the probability of vulnerabilities being exploited increases. That is, given the integrated security countermeasure, we observe that an increase in vulnerability leads to a decrease in SE of PSCs, but an increase in SE of RSCs. Here, we note that this observation is shown under the assumption that the security achieved by RSCs is not equivalent to that of PSCs (for $\alpha = 0.1$). This implies that at some larger level of vulnerability, RSCs are effective to improve the security level of the organization in a decrease of SE of PSCs.

As shown in Fig. 6, SE of the unified security countermeasure increases as vulnerability increases at some lower vulnerabilities. On the contrary, for some higher vulnerabilities, SE of the unified security countermeasure does not increase because SE of PSCs decreases as much as the increase in SE of RSCs. As SE of RSCs, given PSCs, is

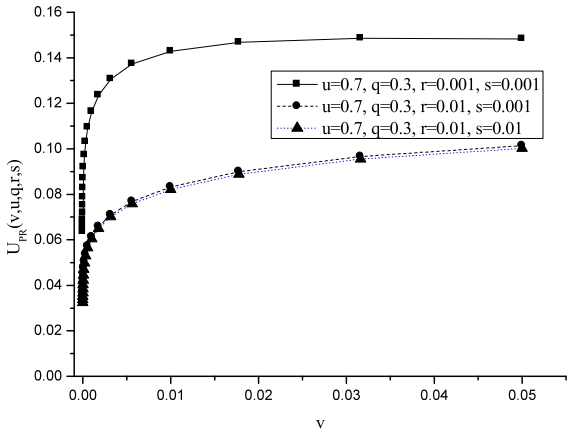

Fig. 6 Influence of v on SE of the unified security countermeasure ($U_{PR}(v, u, q, r, s)$).

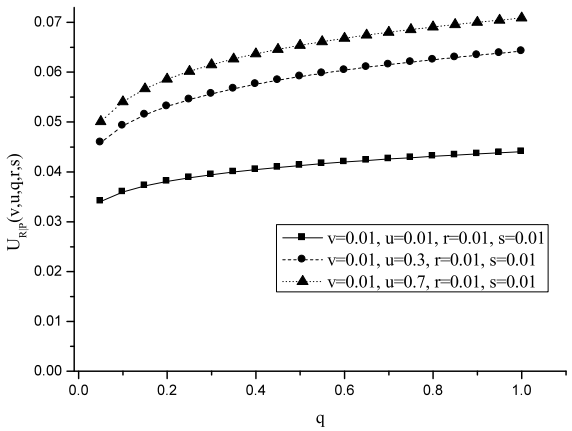

Fig. 7 Influence of q on SE of RSCs ($U_{R|P}(v, u, q, r, s)$).

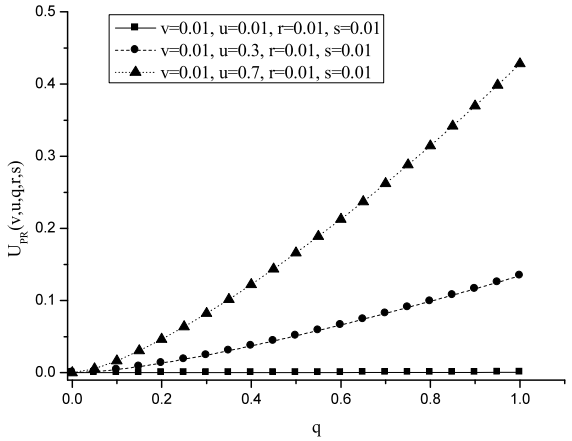

Fig. 8 Influence of q on SE of the unified security countermeasure ($U_{PR}(v, u, q, r, s)$).

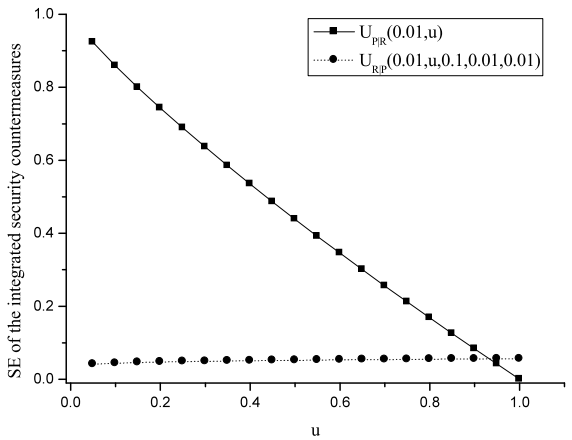

Fig. 9 Influence of u on SE of the integrated security countermeasures ($U_{P|R}(v, u)$ and $U_{R|P}(v, u, q, r, s)$).

mainly affected by the variation in the false positive rate, it is shown that the decrease in the false positive rate (a ten-fold decrease from $r = 0.01$ to $r = 0.001$) is more effective to SE of the unified security countermeasure than that in the false negative rate (a ten-fold decrease from $s = 0.01$ to $s = 0.001$). As mentioned in [7], this implies that for very low base rates, there are more normal events that have a chance of being misclassified as false positive. Even a large change in the false negative rate may not be very beneficial if only a few vulnerabilities are at risk for misclassification as false negative.

4.1.2 Influence of q

In Fig. 7, we show the influence of q on SE of the integrated security countermeasures, given $v = 0.01$, $r = 0.01$, $s = 0.01$ and various values of u: (1) 0.01; (2) 0.3; and (3) 0.7.

For PSCs, we note that their SE does not change depending on the values of q, because PSCs work before vulnerabilities being exploited, i.e., SE of PSCs depends on v and u. On the other hand, it is shown that as q increases, SE of RSCs slowly increases. This is because at some sufficiently larger level of vulnerability exploits, the likelihood that RSCs can classify the potential exploits from the remaining vulnerabilities increases. Also, it is shown that at some higher value of u, SE of RSCs increases. This is because as the value of u increases, the probability that the IT asset is vulnerable after vulnerability elimination increases. That is, given q, at some larger value of vulnerabilities, the likelihood that vulnerabilities are exploited increases and thus, the likelihood that RSCs can classify the potential exploits from the remaining vulnerabilities increases.

As shown in Fig. 8, SE of the unified security countermeasure largely increases as q and u increase. Here, the difference between Figs. 7 and 8 comes from the difference between the input of RSCs, given PSCs, and that of the unified security countermeasure. That is because in case of the unified security countermeasure, SE of PSCs influences on the uncertainty that the system is vulnerable. That is, as u increases, the uncertainty that the system is vulnerable increases. These observations confirm that in an attack dominant situation, the unified security countermeasure is the good candidates to effectively improve the security level of the organization.

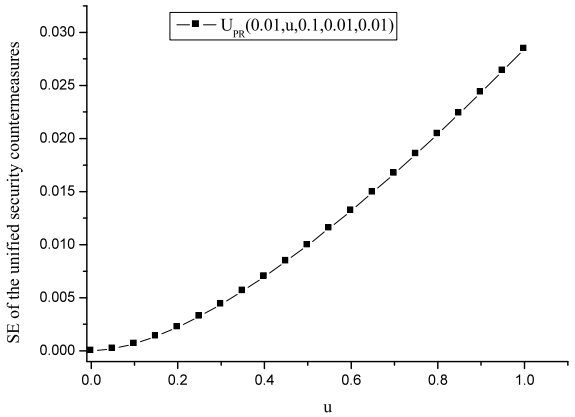

Fig. 10 Influence of u on SE of the unified security countermeasure ($U_{PR}(v, u, q, r, s)$).

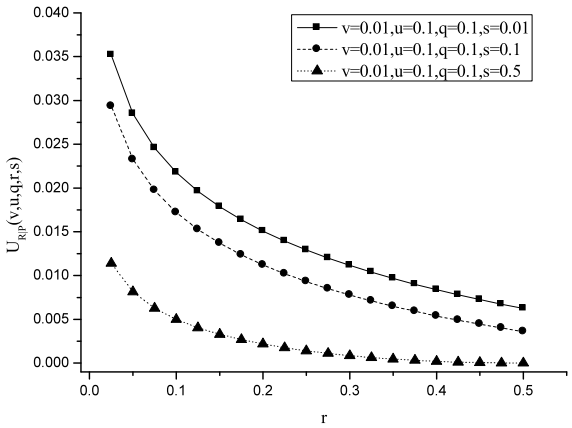

Fig. 11 Influence of r on SE of RSCs.

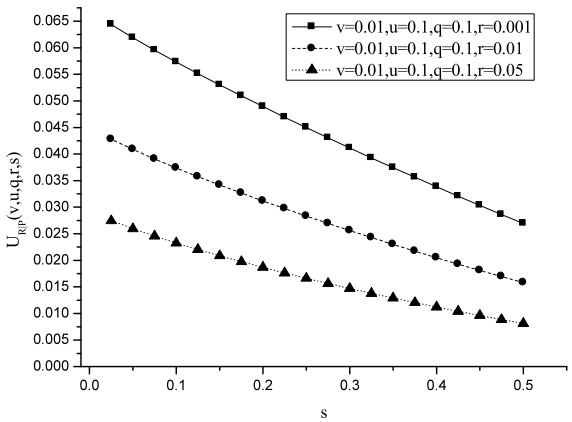

Fig. 12 Influence of s on SE of RSCs.

4.2 Influence of Countermeasure Parameters

Now, we investigate how the change in the probability u of vulnerabilities not being identified affects SE of the integrated security countermeasures and then, how the change in the false positive rate r and the false negative rate s affects their SE. It is shown that a decrease in SE of PSCs can be complemented by an increase in that of their dependent RSCs.

4.2.1 Influence of u

In Fig. 9, we can observe that SE of RSCs is determined by the change in SE of PSCs with respect to the change in the value of u. Here, we assume that $v = 0.01$, $q = 0.1$, $r = 0.01$ and $s = 0.01$. For convenience, we observe the influence of u on the SEs by varying its value from 0.01 to 1.0 in a stepwise manner with step size 0.05.

If PSCs can perfectly eliminate vulnerabilities ($u = 0$), no vulnerabilities are left and thus, SEs of PSCs and RSCs are maximized ($U_{P|R}(v, u) = 1$ and $U_{P|R}(v, u, q, r, s) = 1$). At some sufficiently larger values of u, it is shown that the IT asset becomes vulnerable and thus, SE of PSCs decreases. On the contrary, SE of RSCs increases because the probability of a target asset being vulnerable increases and then, RSCs can classify the potential exploits from the remaining vulnerabilities as exploit or non-exploit. Also, when PSCs do not eliminate vulnerabilities ($u = 1$) at all, SE of PSCs is minimized ($U_{P|R}(v, u) = 0$) and SE of RSCs has a higher value. Also for SE of the unified security countermeasure, as shown in Fig. 10, the SE also increases as u increases, but does not increase much because of the decrease in SE of PSCs. These observations show that by using a unified security countermeasure, a decrease in SE of PSCs can be complemented by an increase in SE of RSCs.

4.2.2 Influence of r and s

In Fig. 11, we show how the false positive rate r affects SE of RSCs, given $\alpha = 0.1$, $v = 0.01$, $u = 0.1$, $q = 0.1$ and various values of s: (1) 0.01; (2) 0.1; (3) 0.5. Here, we vary r from 0.025 to 0.500 in a step wise manner with step size 0.025. It is shown that as the value of r increases, SE of RSCs decreases. This implies that at a higher false positive rate, RSCs may interpret a normal event as a vulnerability exploit. Also, it is shown that at some higher value of s, RSCs has the lower SE. This is because at a higher false negative rate, RSCs may interpret a vulnerability exploit as a normal event.

In Fig. 12, by varying s from 0.025 to 0.500 in a stepwise manner with step size 0.025, we show how the false negative rate s affects SE of RSCs. Here, we assume that $\alpha = 0.1$, $v = 0.01$, $u = 0.1$, $q = 0.1$ and various values of r: (1) 0.001; (2) 0.01; and (3) 0.05. It is shown that as the value of s increases, SE of RSCs decreases. This implies that at a higher false negative rate, the possible exploits resulting from the remaining vulnerability cannot be perfectly classified as non-exploit or exploit by RSCs. As shown in Fig. 11, we observe that at some higher value of r, SE of RSCs decreases because RSCs may interpret a vulnerability non-exploit as a vulnerability exploit. Also, from Figs. 11 and 12, it is shown that the decrease in the false positive rate is more effective to SE of RSCs than that in the false

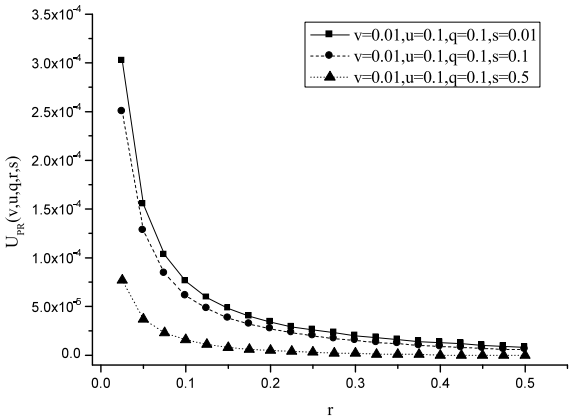

Fig. 13 Influence of r on SE of the integrated security countermeasure ($U_{PR}(v, u, q, r, s)$).

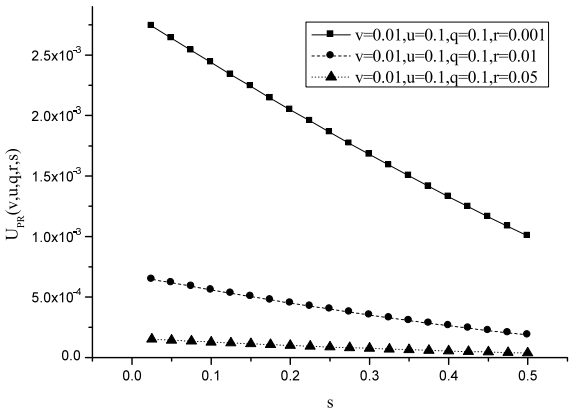

Fig. 14 Influence of s on SE of the integrated security countermeasure ($U_{PR}(v, u, q, r, s)$).

negative rate, as shown in Fig. 5.

As shown in Figs. 13 and 14, SE of the unified security countermeasure decreases as r and s increases. Also, it is shown that as r and s increases, the decrease in SE of the integrated security countermeasures is smaller than the that of RSCs. The difference between Figs. 11 and 13, and Figs. 12 and 14 comes from the difference between the input of RSCs, given PSCs, and that of the unified security countermeasure, as shown in Figs. 7 and 8.

5. Discussion

5.1 How to Determine Values of Security Parameters

To evaluate SE of the integrated security countermeasure by using the proposed model in Fig. 4, we need to determine the values of v, u, q, r and s. By testing the integrated security countermeasures with the well-known attack traces [14], [18], where what data are attacks and what data are normal trace are known, we estimate the values of security parameters, i.e., u, r and s. Also, we estimate v as the number of vulnerabilities of IT assets that can be exploited by attackers to the possible access patterns of the IT asset, and q as the probability of exploits of the given vulnerabilities in the audit data observed by the integrated security countermeasures.

5.2 How to Select the Optimal Configuration against Cost

To show how to select the optimal configuration against cost, we consider the relationship between the capability of the integrated security countermeasure and the amount of investment [19]. For this purpose, we define E_{PR} as the reduction in the organization's expected loss attributable to the capability of the integrated security countermeasure given v. Because known vulnerabilities can be eliminated by the PSCs and the potential exploits of the remaining vulnerabilities can be detected and blocked by the RSCs, we assume that the potential loss associated with the IT asset of v can be reduced in proportion to U_{PR} and thus, E_{PR} can be expressed as:

$$E_{PR}(U_{PR}) = vL \times U_{PR}, \tag{8}$$

where L is the loss associated with the IT asset.

By increasing the investment in security, it is reasonable to expect some decrease in the probability of a breach. In other words, the monetary investment in security to protect the IT asset, denoted as I_{PR}, increases as $U_{PR}(v, u, q, r, s)$ increases. More specifically, we note that the monetary investment in security countermeasures will increase in proportion to the capability of security solutions, but at an increasing rate in the middle of the investment and at a decreasing rate in the beginning of the investment. Thus, we can consider I_{PR} as a function of $U_{PR}(v, u, q, r, s)$, i.e., $I_{PR}(U_{PR}(v, u, q, r, s))$.

The expected net benefits of an investment in the integrated security countermeasures, denoted as $EN_{PR}(U_{PR})$, are the expected benefits resulting from the investment in the integrated security countermeasures minus the monetary investment in security to protect the IT asset. That is, $EN_{PR}(U_{PR})$ is given as the difference between the expected benefits resulting from the investment in the integrated security countermeasures and the monetary investment itself:

$$EN_{PR}(U_{PR}) = E_{PR}(U_{PR}) - I_{PR}(U_{PR}). \tag{9}$$

The nature of the system vulnerability and the capability of security countermeasures lead us to consider the following assumptions concerning $I_{PR}(U_{PR}(v, u, q, r, s))$:

1. $I_{PR}(0) = 0$. It is clear that without the integrated security countermeasures, the investment will remain zero.
2. $I_{PR}(1) = avL$, where 'a' is a measure of the ratio between the loss or potential loss associated with the IT asset and the monetary cost of the integrated security countermeasures. Here, $0 \le a \le 1$ because for an IT asset with vulnerability v, the rational decision maker in the organization will not invest a monetary amount in security that exceeds the loss or potential loss associated with the IT asset of probability v.
3. For all $U_{PR}(v, u, q, r, s)$, $I_{PR}(U_{PR}(v, u, q, r, s))' \ge 0$ and

$I_{PR}(U_{PR}(v,u,q,r,s))'' \geq 0$, where $I_{PR}(U_{PR}(v,u,q,r,s))'$ and $I_{PR}(U_{PR}(v,u,q,r,s))''$ denote the first- and second-order derivatives with respect to $U_{PR}(v,u,q,r,s)$, respectively. We assume that compared to the lower $U_{PR}(v,u,q,r,s)$, the cost of the integrated security countermeasures dramatically increases as $U_{PR}(v,u,q,r,s)$ increases. This assumption views the investment in security as an incremental investment beyond the cost of security countermeasures, specifically their capability.

Based on the above assumptions, we consider an investment function to calculate a closed form countermeasure for the optimal $U_{PR}(v,u,q,r,s)$ and investigate the relationship between the capability of the integrated security countermeasures and the optimal security investment as follows:

$$I_{PR}(U_{PR}) = avL \times U_{PR} \times e^{b \times U_{PR}-1}, \tag{10}$$

where 'b' is a measure of the increase in cost as $U_{PR}(v,u,q,r,s)$ increases. This function is considered because the organization will not invest an excessive amount of money that is larger than vL without security countermeasures and thus, the maximum cost of security countermeasures cannot exceed vL.

Note that from assumption 3, $E_{PR}(U_{PR}(v,u,q,r,s))'' = 0$, $EN_{PR}(U_{PR}(v,u,q,r,s))'' \leq 0$ and thus, $EN_{PR}(U_{PR}(v,u,q,r,s))$ is a concave function. Hence, an interior maximization is characterized by the first order condition with respect to $U_{PR}(v,u,q,r,s)$. That is,

$$\frac{I_{PR}(U_{PR}(v,u,q,r,s))'}{vL} = 1, \tag{11}$$

where the left hand side is the marginal cost of investment (i.e., the cost of increasing $I_{PR}(U_{PR}(v,u,q,r,s))$ by one unit) and the right hand side is the marginal benefit resulting from the security investment in the integrated security countermeasures. Here, we note that $I_{PR}(U_{PR}(v,u,q,r,s))$ measures the monetary investment in security proportional to the capability of the integrated security countermeasures. Based on this assumption, the price of unit of $I_{PR}(U_{PR}(v,u,q,r,s))$ is equal to one, and the marginal cost of investment is also equal to one. Equation (11) means that one should invest in the integrated security countermeasures only up to the point where the marginal benefit is equal to the marginal cost.

As a use case where the organization selects the optimal configuration of the integrated security countermeasure, we now investigate the influence of v and q on the optimal level of investment in the integrated security countermeasure. For $v \in \{0.001, 0.01, 0.1\}$, we vary the value of q from 0 to 1.0 in a stepwise manner with step size 0.05.

In Fig. 15, given v, it is shown that the expected net benefit in the integrated security countermeasure rapidly increases and then decreases at some level of vulnerability exploit as the vulnerability exploit increases. This implies that the capability of the integrated security countermeasure decreases at some higher level of vulnerability exploit and thus, the organization should configure the integrated security countermeasure from the optimal level of investment, i.e., $I^*_{PR}(U_{PR}(v,0.9,q,0.01,0.01))$, where the expected net benefit is maximized. Also, it is shown that the expected net benefit in the integrated security countermeasure increases as v increases from 0.001 to 0.1. This implies that as v increases, expected benefits of an investment in the integrated security countermeasures increases. That is, for the higher value of v, the organization will benefit from the higher investment.

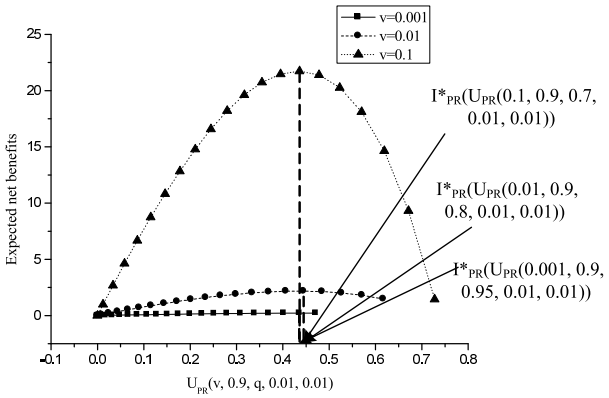

Fig. 15 Influence of the vulnerability exploits on the optimal IT security investment in the integrated security countermeasure.

6. Conclusion

When organizations decide on investment in security, they are interested in minimizing the loss or potential loss resulting from any vulnerabilities in their IT asset. For this purpose, the organizations deploy PSCs or RSCs and then try to increase the security level resulting from the increase of their SEs. To analyze SE of the integrated security countermeasures in different conditions, we proposed a mathematical model in the form of an uncertainty model based on information theory. From the numerical analysis under the influence of controllable and uncontrollable parameters, it was shown that the proposed model is a good alternative for evaluating SE of the integrated security countermeasures.

Acknowledgements

This study was supported by the National Research Foundation of Korea (NRF) grant funded by the Ministry of Science, ICT and Future Planning (MSIP) (NRF-2013R1A1A1005991 and No.2009-0083495).

References

[1] L.A. Gordon, M.P. Loeb, W. Lucyshyn, and R. Richardson, "2005 CSI/FBI Computer Crime and Security Surve," http://americas.utimaco.com/encryption/fbi_csi_2005_P2.html
[2] L.A. Gordon, M.P. Loeb, W. Lucyshyn, and R. Richardson, "2006 CSI/FBI Computer Crime and Security Survey," http://americas.utimaco.com/encryption/fbi_csi_2006_p2.html
[3] I. Ehrlich and G.S. Becker, "Market insurance, self-insurance, and

self-protection," Journal Political Economy, pp.623–648, 1972.
[4] Wikipedia, the free encyclopedia: http://en.wikipedia.org
[5] Rowe, Brent R. and Michael P. Gallaher, Private sector cyber security investment strategies: An empirical analysis, The fifth workshop on the economics of information security (WEIS06), 2006.
[6] R.P. Lippmann, D.J. Fried, I. Graf, J.W. Haines, K.R. Kendall, D. McClung, D. Weber, S.E. Webster, D. Wyschogrod, R.K. Cunningham, and M.A. Zissman, "Evaluating intrusion detection systems: The 1998 DARPA off-line intrusion detection evaluation," Proc. DARPA Information Survivability Conference and Exposition, vol.2, pp.12–26, Jan. 2000.
[7] G. Gu, P. Fogla, D. Dagon, W. Lee, and B. Skori, "Measuring intrusion detection capability: An information-theoretic approach," Proc. 2006 ACM Symposium on Information, computer and communications security, pp.90–101, 2006.
[8] T. Cover and J. Thomas, Elements of Information Theory 2/E, John Wiley & Sons, 2006.
[9] S. Axelsson, "The base-rate fallacy and its implications for the difficulty of intrusion detection," Proc. ACM CCS1999, Nov. 1999.
[10] S. Axelsson, "A preliminary attempt to apply detection and estimation theory to intrusion detection," Technical Report 00-4, Dept. of Computer Engineering, Chalmers Univerity of Technology, Sweden, March 2000.
[11] D. Denning, "An intrusion-detection model," IEEE Trans. Softw. Eng., vol.13, no.2, pp.222–232, Feb. 1987.
[12] P. Helman and G. Liepins, "Statistical foundations of audit trail analysis for the detection of computer misuse," IEEE Trans. Softw. Eng., vol.19, no.9, pp.886–901, Sept. 1993.
[13] J. Hancock and P. Wintz, Signal Detection Theory, McGraw-Hill, 1966.
[14] R.P. Lippmann, D.J. Fried, I. Graf, and J.W. Haines, "Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation," Proc. 2000 DARPA Information Survivability Conference and Exposition (DISCEX00), 2000.
[15] J. McHugh, "Testing intrusion detection systems: A critique of the 1998 and 1999 darpa off-line intrusion detection system evaluation as performed by lincoln laboratory," ACM Trans. Information and System Security, vol.3, no.4, pp.262–294, Nov. 2000.
[16] J.E. Gaffney and J.W. Ulvila, "Evaluation of intrusion detectors: A decision theory approach," Proc. 2001 IEEE Symposium on Security and Privacy, pp.50–61, May 2001.
[17] E. Ciapessoni, D. Cirio, S. Grillo, S. Massucco, A. Pitto, and F. Silvestro, "An integrated platform for power system security assessment implementing probabilistic and deterministic methodologies," Systems Journal, vol.7, no.4, pp.845–853, 2013.
[18] INFOFUSE: The DEFCON "capture the flag," data set: http://cs.uccs.edu/~infofuse/src/inside_dump, 1999.
[19] Y.-H. Choi, "A framework for makin decision on optimal security investment to the proactive and reactive security solutions," KSII J. Internet Computing and Services, vol.15, no.3, pp.91–100, June 2014.

Yoon-Ho Choi is a faculty member at the School of Computer Science and Engineering in Pusan National University, Busan, Korea. He received his M.S. and Ph.D. degrees from the School of Electrical and Computer Engineering, Seoul National University, S. Korea, in Aug. 2004 and Aug. 2008, respectively. He was a postdoctoral scholar at Seoul National University, Seoul, S. Korea from Sept. 2008 to Dec. 2008 and in Pennsylvania State University, University Park, PA, USA from Jan. 2009 to Dec. 2009. He worked as a senior engineer at Samsung Electronics from May 2010 to Feb. 2012. He has served as a TPC member in various international conferences and journals. His research interests include Deep Packet Inspection (DPI) for high-speed intrusion prevention, mobile computing security, vehicular network security for realizing secure computers and networks.

Han-You Jeong is a faculty member at the Department of Electrical Engineering in Pusan National University, Busan, Korea. He received the B.S., M.S., and Ph.D. degrees in the Department of Electrical Engineering and Computer Science from Seoul National University, Seoul, Korea, in 1998, 2000, and 2005, respectively. From 2005 to 2007, he was a senior engineer with the Telecommunication R&D Center, Samsung Electronics, Suwon, Korea. In 2008, he joined the Digital Technology Center, University of Minnesota, Minneapolis, as a postdoctoral research fellow. He is an associate professor at Pusan National University (PNU), and currently leads the Networked Smart Systems Laboratory (NSSLab), PNU, Busan, Korea. His research interests include wireless networks, vehicular networks, and optical networks.

Seung-Woo Seo is the professor at the School of Electrical Engineering in Seoul National University, Seoul and Director of Intelligent Vehicle IT (IVIT) Research Center funded by Korean Government and Automotive Industries. He received his Ph.D. from Pennsylvania State University, University Park, USA, and B.S. and M.S. degrees from Seoul National University, Seoul, Korea, and all in Electrical Engineering. He was with the Faculty of the Department of Computer Science and Engineering, Pennsylvania State University, and served as a Member of the Research Staff in the Department of Electrical Engineering in Princeton University, Princeton, NJ. In 1996, he joined the Faculty of the School of Electrical Engineering and the Institute of New Media and Communications in Seoul National University. He has served as Chair or a Committee Member in various international conferences and workshops including INFOCOM, GLOBECOM, PIMRC, VTC, MobiSec, Vitae, etc. He also served for five years as a Director of the Information Security Center in Seoul National University. His research areas include vehicular electronics for intelligent vehicles, communication networks, computer & network security, and system optimization.