# Influence of Defensive Actions on Security Metrics Values

Leanid Krautsevich and Artsiom Yautsiukhin

Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche,
Via G. Moruzzi 1, Pisa 56124, Italy
{leanid.krautsevich,artsiom.yautsiukhin}@iit.cnr.it

**Abstract.** Security management requires quantitative security indicators, called security metrics, in order to effectively distribute limited resources and justify investments into security. The problem is not only to select the security metrics, but also to be sure that the metrics correctly represent security strength.
In this paper, we tackle the problem of formal analysis of different quantitative security metrics. We consider a formal model which is based interactions between an attacker and a system. We use model in order to define security metrics and defensive actions which supposed to improve security strength of a system. We exploit definitions to analyse whether security metrics are able to indicate these improvements correctly.

## 1 Introduction

Security metrics attract the attention of the security community for more that twenty years [3, 7]. However, the field is still missing a general formal model which is capable of describing security metrics [6]. Such model should provide a theoretical background which allows formal analysis of security metrics. This analysis is required to prove that metrics can be used as reliable indicators for security strength.

Recently, we presented first steps towards a model that allows formal definition and analysis of quantitative security metrics, e.g., the number of attacks existing to a system [9, 10]. In our model we exploited findings of the measurement theory which defines the conditions (known as representation theorem) which formally state when a metric can be considered as a proper indicator for some quality of an object [2, 20]. We showed, that in order to apply the findings of the measurement theory to security metrics we must define the empirical "more secure" relation for systems and only then we are able to check whether a metric correctly represents security of the system. We also introduced a criterion which is based on a simple, but evident assumption, that a system with the same possible attacks as another system cannot be more secure than the second one. This criterion allowed us to check whether the formalised metrics correctly represent the relation between two systems in terms of security strength.

In these papers we extended our work analysing the behaviour of the security metrics in response to defensive actions applied by a security administrator. In

fact, we formally define the ways how security of a system can be enhanced. We call the ways defensive actions and analyse how security metrics values changes when defensive actions are applied.

The rest of the paper goes as follows. Section 2 recalls the details of our basic formal model. Section 3 presents the definitions of several general security metrics from our previous work. Section 4 introduces the defensive actions and analyses their impact on the values of security metrics. Section 5 describes the related work. The conclusion is presented in Section 6

## 2 Formal Model

We recall important peculiarities of our formal model [9, 10] that allows a more accurate discussion about security metrics. The target of our analysis is a system which is applied out of a context, i.e., we do not consider preferences of attackers and possible impact of attacks. We use the notation of the process algebra [17] and define a perfect security as:

**Definition 1.** *Let $S$ be a process modelling behaviour of a system and $X$ a process modelling behaviour of an attacker. The system and the attacker perform actions $a_i \in A_S$ and $a_j \in A_X$ correspondingly and move from one state to another one (different states of the same process are denoted with different amount of primes, e.g., $S, S', S''$). We denote a trace of actions accomplished by the system $\gamma_S$ and by the attacker as $\gamma_X$. A trace $\gamma = \gamma_S \bullet \gamma_X$ is a result of merging one trace of actions with another one in a way that preserves the order of events. We say that the system $S$ is (perfectly) secure if and only if:*

$$\forall X, \gamma = \gamma_S \bullet \gamma_X, \gamma_S \in S, \gamma_X \in X, S \xrightarrow{\gamma_S} S' \wedge X \xrightarrow{\gamma_X} X', \quad (1)$$
$$S \| X \xrightarrow{\gamma} S' \| X' \Rightarrow \mathscr{P}_{sec}(S' \| X') = \emptyset$$

Function $\mathscr{P}_{sec}(S' \| X')$ returns the set of possible goals successfully achieved by an attacker in the state $S' \| X'$ (e.g., the attacker has root access to a database) when the system and the attacker work in parallel. Equivalence to the empty set means that no goals are successfully achieved, i.e., the security [5] is preserved. We write $\gamma_X \in X$ to show that the attacker may execute a trace of actions and $\gamma_S \in S$ to show that the system may execute a trace of actions. A trace of actions is denoted in the following way preserving the order of actions: $\gamma = a_1 \circ a_2 \circ \cdots \circ a_n$. We use the same operator to show that a sequence follows another sequence $\gamma = \gamma_1 \circ \gamma_2$. We use $a \in \gamma$ notation to denote that an action $a$ is contained in the trace $\gamma$.

**Definition 2.** *An attack to a system $S$ is a trace of actions $\gamma_X$:*

$$\exists X, \gamma = \gamma_S \bullet \gamma_X, \gamma_S \in S, \gamma_X \in X, S \xrightarrow{\gamma_S} S' \wedge X \xrightarrow{\gamma_X} X', \quad (2)$$
$$S \| X \xrightarrow{\gamma} S' \| X' \Rightarrow \mathscr{P}_{sec}(S' \| X') \neq \emptyset$$

Thus, the attack is the trace of actions of an attacker that leads to a state where the attacker reaches her goal (set of goals). Now we define a set of attacks relevant to a system.

**Definition 3.** *Let $\mathcal{X}_S$ be a set of all attackers relevant to a system $S$. The sets of attacks relevant to system $S$ is:*

$$\begin{aligned} \Gamma_X(S) := \{\gamma_X : \gamma = \gamma_S \bullet \gamma_X, \gamma_S \in S, \gamma_X \in X, X \in \mathcal{X}_S, \\ S \xrightarrow{\gamma_S} S' \wedge X \xrightarrow{\gamma_X} X', S\|X \xrightarrow{\gamma} S'\|X' \Rightarrow \mathscr{P}_{sec}(S'\|X') \neq \emptyset\} \end{aligned} \tag{3}$$

We derive a criterion that determines the "more secure" relation.

**Criterion 1** *Let $\Gamma_{S_1}$ be a set of attacks relevant to a system $S_1$ and $\Gamma_{S_2}$ be a set of attacks relevant for a system $S_2$. We say that the system $S_1$ is more secure than or equally secure to the system $S_2$ ($S_1 \succeq_{sec} S_2$) if a set of attacks $\Gamma_{S_1}$ relevant to the system $S_1$ is included into a set of attacks $\Gamma_{S_2}$ relevant to the system $S_2$ ($\Gamma_{S_1} \subseteq \Gamma_{S_2}$). Formally:*

$$S_1 \succeq_{sec} S_2 \; if \; \Gamma_{S_1} \subseteq \Gamma_{S_2} \tag{4}$$

Criterion 1 does not allow distinguishing between equal or higher security in case $\Gamma_{S_1} \subset \Gamma_{S_2}$ thus we call this definition *non sensitive*. The *sensitive* definitions can be formalised in the following way. Formally,

**Criterion 2** *We say that the system $S_1$ is more secure than the system $S_2$ ($S_1 \succ_{sec} S_2$) if a set of attacks $\Gamma_{S_2}$ relevant to the system $S_2$ is wider that the set of attacks $\Gamma_{S_1}$ for system $S_1$ ($\Gamma_{S_1} \subset \Gamma_{S_2}$):*

$$S_1 \succ_{sec} S_2 \; if \; \Gamma_{S_1} \subset \Gamma_{S_2} \tag{5}$$

*We say that the system $S_1$ is equally secure to the system $S_2$ ($S_1 \sim_{sec} S_2$) if a set of attacks $\Gamma_{S_1}$ relevant to the system $S_1$ is equal to a set of attacks $\Gamma_{S_2}$ relevant to the system $S_2$ ($\Gamma_{S_1} = \Gamma_{S_2}$). Formally,*

$$S_1 \sim_{sec} S_2 \; if \; \Gamma_{S_1} = \Gamma_{S_2} \tag{6}$$

Naturally, Criteria 1 and 2 can be applied only for a very limited amount of real systems we used this criteria since it is a trivial one. We have shown that many metrics satisfy one of the two criteria in [9] and extended the analysis with context-based metrics in [10].

More sophisticated criteria are required for more precise analysis of security metrics. The problem is that such sophisticated criteria are often arguable and may be rejected by some security experts. Nevertheless, in this paper we try to move slightly forward and improve our criteria with another trivial amendment.

## 3 Definitions of Metrics

In this section, we present formal definitions for several general quantitative security metrics. For a metric $\mathscr{M}$ we write $\mathscr{M}(S)$ to denote that the metric is computed for a system $S$, e.g., for a workstation with all hardware and software installed.

Measurement theory defines the following theorem for correct assessment of an empirical system metrics must satisfy the representation theorem [20, 2], which in our case may be seen as follows:

**Definition 4.** *Let $S_1$ and $S_2$ be two systems of type $\mathcal{S}$ and $\mathscr{M} : \mathcal{S} \mapsto \mathbb{R}$ be an objective-empirical function which assigns a real value to an element from $\mathcal{S}$. Then:*

$$S_1 \succeq_{sec} S_2 \Leftrightarrow \mathscr{M}(S_1) \succeq_{\mathscr{M}} \mathscr{M}(S_2) \tag{7}$$

Where $\mathscr{M}(S_1) \succeq_{\mathscr{M}} \mathscr{M}(S_2)$ means that $\mathscr{M}(S_1)$ is better than or equal to $\mathscr{M}(S_2)$ (e.g., the number of attacks for $S_1$ is less than for $S_2$).

In the literature the metrics are introduced in such a way to define this relation only in one way (e.g., better metrics means better security). In this paper we would like to consider possible proves in the opposite way.

*Number of attacks.* Number of attacks metric defines how many attacks on a system exist. The idea behind this metric is that the more attacks for a system exist the less secure the system is. This metric is applied for the simplest analysis of attack graphs [18, 19]. Number of attacks also can be used for the analysis of results of the penetration testing.

**Definition 5.** *Number of attacks $N_{att}(S)$:*

$$N_{att}(S) = |\Gamma_X(S)| \tag{8}$$

The last line of Definition 5 leaves only the minimal sequences of attack steps, i.e., only essential steps for an attack are considered.

**Criterion 3** *Number of attacks is a suitable metric for security of a system considered out of a context.*

$$S_1 \succeq_{sec} S_2 \Rightarrow N_{att}(S_1) \leq N_{att}(S_2) \tag{9}$$

*Minimal cost of attack.* Minimal cost of attack represents the minimal cost the attacker have to pay for the execution of an attack to a system [19].

We start with the definition of cost $C(\gamma_X)$ of the attack $\gamma_X$. Let $C(a)$ be the cost of the execution of the action $a \in \gamma_X$ of the attack $\gamma_X$.

**Definition 6.** *Cost of attack $C(\gamma_X)$ is:*

$$C(\gamma_X) = \sum_{\forall a \in \gamma_X} C(a), \gamma_X = a_1 \circ a_2 \circ \cdots \circ a_n \tag{10}$$

**Definition 7.** *Minimal cost of attack* $C^{min}(S)$*:*

$$C^{min}(S) = \min_{\forall \gamma_X \in X} \{C(\gamma_X) : \gamma_X \in \Gamma_X(S)\} \tag{11}$$

**Criterion 4** *Minimal cost of attack is a suitable metric for security of a system considered out of a context.*

$$S_1 \succeq_{sec} S_2 \Rightarrow C^{min}(S_1) \geq C^{min}(S_2) \tag{12}$$

*Shortest Length of Attacks.* An intuition behind this metric is the following: the less steps an attacker has to make, the simpler is to execute the attack successfully, and the less secure the system is [18]. We start with the definition of an attack length:

**Definition 8.** *The length* $L(\gamma_X)$ *of attacks* $\gamma_X$ *is:*

$$L(\gamma_X) = |\gamma_X|, \gamma_X \in \Gamma_X(S) \tag{13}$$

*We slightly abuse the notation using* $|\gamma_X|$ *to determine the number of steps in a sequence.*

**Definition 9.** *The shortest length of attacks* $L^{min}(S)$ *is:*

$$L^{min}(S) = \min_{\forall \gamma_X \in X} \{L(\gamma_X) : \gamma_X \in \Gamma_X(S)\} \tag{14}$$

**Criterion 5** *Shortest length of attacks is a suitable metric for security of a system considered out of a context.*

$$S_1 \succeq_{sec} S_2 \Rightarrow L^{min}(S_1) \geq L^{min}(S_2) \tag{15}$$

*Maximal probability of successful attack.* The probability to accomplish an attack successfully is a well-known metric [23]. The metric describes the most probable way to compromise the system.

We start with the definition of probability of attack to be successful $\mathbf{Pr}(\gamma_X)$ of the attack $\gamma_X$. Let $\mathbf{Pr}(a)$ be the probability of the execution of the action $a \in \gamma_X$.

**Definition 10.** *Probability* $\mathbf{Pr}(\gamma_X)$ *of a successful attack is:*

$$\mathbf{Pr}(\gamma_X) = \prod_{\forall a \in \gamma_X} \mathbf{Pr}(a), \gamma_X = a_1 \circ a_2 \circ \cdots \circ a_n,\ \gamma_X \in \Gamma_X(S) \tag{16}$$

*We assumed that the attack actions are independent.*

**Definition 11.** *We define maximal probability of successful attack as follows:*

$$\mathbf{Pr}^{max}(S) = \max_{\forall \gamma_X \in X} \{\mathbf{Pr}(\gamma_X) : \gamma_X \in \Gamma_X(S)\} \tag{17}$$

**Criterion 6** *Maximal probability of attack is a suitable metric for security of a system considered out of a context.*

$$S_1 \succeq_{sec} S_2 \Rightarrow \mathbf{Pr}^{max}(S_1) \leq \mathbf{Pr}^{max}(S_2) \tag{18}$$

*Attack surface metric.* This metric has been proposed by Howard [4] and Manadhata and Wing [13]. Here we consider one of the latest versions of attack surface metric presented by Manadhata et al., [15, 16]

**Definition 12.** *Let us have three assets which can be affected by an attack:* method (m), data items (d), channel (c). *Let us know the damage-potential level* $dmg_{pot}(\gamma_X)$ *of every asset and the level of privileges* $priv(\gamma_X)$ *required for execution of an attack* $\gamma_X$ *(maximal difference in level of privileges among required actions of the same attack). For every system we can assign the following tuple:*

$$ASM(S) = \langle Risk^m, Risk^c, Risk^d \rangle \tag{19}$$

*where*

$$Risk^m = \sum_{\forall \gamma_X \in \Gamma^m} \frac{dmg_{pot}(\gamma_X)}{priv(\gamma_X)};\ Risk^c = \sum_{\forall \gamma_X \in \Gamma^c} \frac{dmg_{pot}(\gamma_X)}{priv(\gamma_X)}; \tag{20}$$
$$Risk^d = \sum_{\forall \gamma_X \in \Gamma^d} \frac{dmg_{pot}(\gamma_X)}{priv(\gamma_X)}$$

*where* $\Gamma^m, \Gamma^c, \Gamma^d$ *are the sets of attacks leading to compromise of the corresponding asset.*

**Criterion 7** *Attack surface is a suitable metric for security of a system considered out of a context.*

$$S_1 \succeq_{sec} S_2 \Rightarrow ASM(S_1) \leq ASM(S_2) \tag{21}$$

## 4 Defensive Actions

If we consider all possible states as nodes and possible actions performed by the system and an attacker as edges, we can construct an attack graph [8, 18]. The attack graph $G = (V, A)$ is the set $S$ of nodes representing vulnerabilities in the system and the set of edges $A$ representing attempts (attack steps $a$) to execute the vulnerabilities. Successful execution of a vulnerability gives new privileges to the attacker. Some nodes of the attack graph denote the states, where some attacker goal is achieved ($\mathscr{P}_{sec}(S \| X) \neq \emptyset$).

System can be modified in several ways. For example, security patches are installed, new services become available, access rules are changed, accounts deleted, etc. Such modifications change the system, and thus, its behaviour. Moreover, they may affect the behaviour of an attacker. In order to model such changes of the system, we first define simplest modifications similar to the ones specified for graphs [1]:

- insert action,
- insert state,
- delete action,

– delete state,
– change labels.

Naturally, the defensive actions should make the attacks harder to perform successfully. Therefore, we need to consider such modifications, which have only positive effect on security of the system. Thus, we define simplest defensive actions.

**Definition 13.** *Let $S||X \stackrel{d}{\Longrightarrow} \hat{S}||\hat{X}$ means the transformation of a system $S$ to a system $\hat{S}$ and an attacker $X$ to an attacker $\hat{X}$ after applying an action $d$. We formally define the simplest defensive actions $d \in D_s$ as follows.*

– delete an action $a$:

$$\begin{aligned}
&\exists a \in \gamma = \gamma_S \bullet \gamma_X, \gamma_X \in \Gamma_X(S) \ . \ S||X \xrightarrow{\gamma} S^*||X^* \ \mathscr{P}_{sec}(S^*||X^*) \neq \emptyset \ \wedge \\
&S||X \xrightarrow{a} S'||X' \ \wedge \ \nexists a \ . \ \hat{S}||\hat{X} \xrightarrow{a} \hat{S}'||\hat{X}' \ \wedge \\
&\forall a' \neq a \ . \ S''||X'' \xrightarrow{a'} S'''||X''' \ \wedge \ \exists a' \ . \ \hat{S}''||\hat{X}'' \xrightarrow{a'} \hat{S}'''||\hat{X}'''
\end{aligned} \tag{22}$$

– delete state $S'||X'$:

$$\begin{aligned}
&\forall a, a' \in \gamma = \gamma_S \bullet \gamma_X, \gamma_X \in \Gamma_X(S) \ . \ S||X \xrightarrow{\gamma} S^*||X^* \ \mathscr{P}_{sec}(S^*||X^*) \neq \emptyset \ \wedge \\
&S||X \xrightarrow{a} S'||X' \ \wedge \ S'||X' \xrightarrow{a'} S''||X'' \ \wedge \\
&\nexists a, a' \ . \ \hat{S}||\hat{X} \xrightarrow{a} \hat{S}'||\hat{X}' \ \wedge \ \hat{S}'||\hat{X}' \xrightarrow{a'} \hat{S}''||\hat{X}'' \ \wedge \\
&\forall a'' \neq a, a' \ . \ S'''||X''' \xrightarrow{a''} S''''||X'''' \ \wedge \ \exists a'' \ . \ \hat{S}'''||\hat{X}''' \xrightarrow{a''} \hat{S}''''||\hat{X}''''
\end{aligned} \tag{23}$$

– substitute action $a$ with action $\hat{a}$; such that for any label $Lab$:

$$\begin{aligned}
&\exists a \in \gamma = \gamma_S \bullet \gamma_X, \gamma_X \in \Gamma_X(S) \ . \ S||X \xrightarrow{\gamma} S^*||X^* \ \mathscr{P}_{sec}(S^*||X^*) \neq \emptyset \ \wedge \\
&S||X \xrightarrow{a} S'||X' \ \ \nexists a \ . \ \hat{S}||\hat{X} \xrightarrow{a} \hat{S}'||\hat{X}' \ \exists \hat{a} \ . \ \hat{S}||\hat{X} \xrightarrow{\hat{a}} \hat{S}'||\hat{X}' \ \wedge \\
&\nexists \hat{a} \ S||X \xrightarrow{\hat{a}} S'||X' \ Lab(\hat{a}) \succeq_{\mathscr{M}} Lab(a) \ \wedge \\
&\forall a' \neq a \ . \ S''||\hat{X}'' \xrightarrow{a'} S'''||X''' \ \wedge \ \exists a' \neq \hat{a} \ . \ \hat{S}''||\hat{X}'' \xrightarrow{a'} \hat{S}'''||\hat{X}'''
\end{aligned}$$

– substitute action $a$ with one state and two actions $\hat{a}$ and $\hat{a}'$ such that $\hat{a}$ start at the same stage that $a$ starts and ends at the new state and $\hat{a}'$ connects this state with the state to which action $a$ leads, thus, for all $Lab$:

$$\begin{aligned}
&\exists a \in \gamma = \gamma_S \bullet \gamma_X, \gamma_X \in \Gamma_X(S) \ . \ S||X \xrightarrow{\gamma} S^*||X^* \ \mathscr{P}_{sec}(S^*||X^*) \neq \emptyset \ \wedge \\
&S||X \xrightarrow{a} S'||X' \ \wedge \ \nexists a \ . \ \hat{S}||\hat{X} \xrightarrow{a} \hat{S}'||\hat{X}' \ \wedge \\
&\exists \hat{a}, \hat{a}' \ . \ \hat{S}||\hat{X} \xrightarrow{\hat{a}} \hat{S}'||\hat{X}' \ \wedge \ \hat{S}'||\hat{X}' \xrightarrow{\hat{a}'} \hat{S}''||\hat{X}'' \ \wedge \\
&\nexists \hat{a}, \hat{a}' \ . \ S||X \xrightarrow{\hat{a}} S'||X' \ \wedge \ S'||X' \xrightarrow{\hat{a}'} S''||X'' \ \wedge Lab(\hat{a} \circ \hat{a}') \succeq_{sec} Lab(a) \\
&\forall a' \neq a \ . \ S'''||X''' \xrightarrow{a'} S''''||X'''' \ \wedge \ \exists a' \ . \ \hat{S}'''||\hat{X}''' \xrightarrow{a'} \hat{S}''''||\hat{X}''''
\end{aligned} \tag{24}$$

We would like to note, that defensive actions and ordinary actions have different affect on the process. Ordinary actions simply move a process from one state to another, but the process itself is left the same, i.e., it has the same actions and states. Defensive actions modify the process, but have no effect on the current state of the process. The reasoning in equivalent to the graphs. One may consider a walk through the graph as moving from a state to a state. But, such change differs from removing parts of the graph from considerations (e.g., a cut).

In Definition 13 we considered processes with hats (e.g., $\hat{S}$) as the same processes without hats $S$, but the ones we have after applying a simplest defensive action. Although, we acknowledge, that some defensive actions may affect only a system, when others affect only an attacker, we consider both processes changed, for brevity. Thus, in some cases one of the processes will be the same (e.g., if we remove an action of a system $X = \hat{X}$). We do the same for changing a state in the definitions. In the definition we also used processes marked with a star (e.g., $S^*||X^*$ to denote a state of the process. In fact, in the definitions, this is a compromised state.

**Proposition 1.** $\forall d \in D_s \; \forall S, \hat{S} \; . \; S \overset{d}{\Longrightarrow} \hat{S} \Longrightarrow |\Gamma_X(S)| \geq |\Gamma_X(\hat{S})|$

*Proof.* In the following proofs, the attacks not affected by simple defensive actions will be relevant for both systems: before applying the defensive action $S$ and after $\hat{S}$. This follows from the last statements in all definitions of simple defensive actions, that all actions not affected by the change are relevant for $\hat{S}$. Thus, in the following we focus only on the changed part:

- delete an action. Since the deleted action belongs to at least one sequence which leads to a compromised state and includes an attack $a \in \gamma = \gamma_S \bullet \gamma_X, \gamma_X \in \Gamma_X(S)$ these attacks $\gamma \notin \Gamma(\hat{S})$. Thus, $\Gamma_X(\hat{S}) \subset \Gamma_X(S)$
- delete a state. If we delete a state we delete two actions and the proof is the same as for deleting an action.
- substitute action $a$ with action $\hat{a}$. This means that $\forall \gamma = \gamma_S \bullet \gamma_X = \gamma_1 \circ a \circ \gamma_3, \gamma_X \in \Gamma_X(S) \; \exists \hat{\gamma} = \gamma_1 \circ \hat{a} \circ \gamma_3 \in \Gamma_X(\hat{S})$. Thus, $|\Gamma_X(\hat{S})| = |\Gamma_X(S)|$.
- substitute action $a$ with one state and two actions $\hat{a}$ and $\hat{a}'$. Similar to the previous observation, this means that $\forall \gamma = \gamma_S \bullet \gamma_X = \gamma_1 \circ a \circ \gamma_3, \gamma_X \in \Gamma_X(S) \; \exists \hat{\gamma} = \gamma_1 \circ \hat{a} \circ \hat{a}' \circ \gamma_3 \in \Gamma_X(S)$. Since the rule states, that other actions are left the same and the added state did not exist for $S$, thus, no other actions lead to or from this state. Therefore, $|\Gamma_X(\hat{S})| = |\Gamma_X(S)|$.

Defensive actions ($D$) can be considered as some combination of simple defensive actions. This means that we assume, that all actions are applied correctly, i.e., no additional threats (additional actions, states, etc) are added because of incorrectly performed defensive actions. We also assume that defensive actions do not conflict with each other.

### 4.1 Effect of defensive actions on metrics

The security actions supposed to make system more secure. Thus, we propose a new criterion, which extends Criteria 1 and 2:

**Criterion 8** $\hat{S} \succeq_{sec} S \; if \; \forall d \in D \; \forall S, \hat{S} \; . \; S||X \stackrel{d}{\Longrightarrow} \hat{S}||\hat{X}$

Now we would like to check whether the security metrics are compatible with Criterion 8. Since, for the defensive actions related to removing action or a state we have shown that $\Gamma_X(\hat{S}) \subseteq \Gamma_X(S)$, and for this condition we have shown that metrics are capable to detect it in [9] there is no need for us to consider this part again.

*Number of attacks*

**Proposition 2.** $\forall d \in D_s \; \forall S, \hat{S} \; . \; S||X \stackrel{d}{\Longrightarrow} \hat{S}||\hat{X} \Longrightarrow N_{att}(S) \geq N_{att}(\hat{S})$

*Proof.* From Proposition 1 we see that $|\Gamma_X(S)| = N_{att}(S) \geq N_{att}(\hat{S}) = |\Gamma_X(\hat{S})|$. Note, that if we improve security with a defensive action which substitutes ones action with another one we have, that $N_{att}(S) = N_{att}(\hat{S})$.

*Minimal cost of attacks*

**Proposition 3.** $\forall d \in D_s \; \forall S, \hat{S} \; . \; S||X \stackrel{d}{\Longrightarrow} \hat{S}||\hat{X} \Longrightarrow C_{att}^{min}(S) \leq C_{att}^{min}(\hat{S})$

*Proof.* Since the third and the fourth simple defensive actions state that $Lab(\hat{a}) \succeq_{\mathscr{M}} Lab(a)$ and $Lab(\hat{a} \circ \hat{a}') \succeq_{sec} Lab(a)$, this means that $C(\hat{a}) \geq C(a)$ and $C(\hat{a} \circ \hat{a}') \geq C(a)$. Thus, if the cost of the attack before the system update was $C(\gamma)$, then now it is $C(\gamma) < C(\gamma) + C(\hat{a}) - C(a) \; \forall \gamma = \gamma_1 \circ a \circ \gamma_3$. Thus, $C_{att}^{min}(\hat{S}) \geq C_{att}^{min}(S)$

*Shortest length of attacks*

**Proposition 4.** $\forall d \in D_s \; \forall S, \hat{S} \; . \; S||X \stackrel{d}{\Longrightarrow} \hat{S}||\hat{X} \Longrightarrow L^{min}(S) \leq L^{min}(\hat{S})$

*Proof.* The defensive action three does not change the length of any attack, while the fourth one increases it by 1, substituting one step with two. Thus, $L^{min}(S) \leq L^{min}(\hat{S})$.

*Maximal probability of attacks*

**Proposition 5.** $\forall d \in D_s \; \forall S, \hat{S} \; . \; S \stackrel{d}{\Longrightarrow} \hat{S} \Longrightarrow \mathbf{Pr}^{max}(S) \geq \mathbf{Pr}^{max}(\hat{S})$

*Proof.* Since the third and the fourth simple defensive actions state that $Lab(\hat{a}) \succeq_{\mathscr{M}} Lab(a)$ and $Lab(\hat{a} \circ \hat{a}') \succeq_{sec} Lab(a)$, this means that $\mathbf{Pr}(\hat{a}) \leq \mathbf{Pr}(a)$ and $\mathbf{Pr}(\hat{a} \circ \hat{a}') \leq \mathbf{Pr}(a)$. Thus, if the cost of the attack before the system update was $\mathbf{Pr}(\gamma)$, then now it is $\mathbf{Pr}(\gamma) < \mathbf{Pr}(\gamma) * \mathbf{Pr}(\hat{a})/\mathbf{Pr}(a) \; \forall \gamma = \gamma_1 \circ a \circ \gamma_3$. Thus, $\mathbf{Pr}^{max}(S) \geq \mathbf{Pr}^{max}(\hat{S})$

*Attack surface*

**Proposition 6.** $\forall d \in D_s\ \forall S, \hat{S}\ .\ S||X \stackrel{d}{\Longrightarrow} \hat{S}||\hat{X} \Longrightarrow ASM(S) \geq ASM(\hat{S})$

*Proof.* In [9] we considered an old version of attack surface metric. Since, here we use the new one, we also need to prove the proposition for the first two simplest defensive actions. Since both of them result in a strict $\Gamma_X(\hat{S}) \subset \Gamma_X(S)$ relation this results in smaller number of non-negative summands for $Risk^m$, $Risk^c$, or $Risk^d$ and the value of some of these risks reduces (while non-affected risk values are left the same). Thus, $ASM(\hat{S}) < ASM(S)$.

Since the third and the fourth simple defensive actions state that $Lab(\hat{a}) \succeq_{\mathscr{M}} Lab(a)$ and $Lab(\hat{a} \circ \hat{a}') \succeq_{sec} Lab(a)$, this means that $priv(\hat{a}) \geq priv(a)$ and $priv(\hat{a} \circ \hat{a}') \geq priv(a)$. Thus, the privilege levels for the attacks including these steps: $priv(\hat{\gamma}) \geq priv(\gamma)(\forall \gamma \in \Gamma_X(S)\ .\ a \in \gamma\ \wedge\ \forall \hat{\gamma} \in \Gamma_X(\hat{S})\ .\ \hat{a} \in \hat{\gamma})$. Therefore, $ASM(S) \geq ASM(\hat{S})$

We see that all metrics are able to correctly indicate the defensive actions applied in a system. In our previous work [9] we have shown, that only the number of attacks metric satisfy the sensitive Criterion 2, when other metrics satisfy non-sensitive Criterion 1. Here we have shown that the number of attacks cannot detect improvement of security strength caused by the defensive action which substitutes an action. Thus, the new assumption about more secure relation (Criterion 8) shows, that all metrics are non-sensitive.

## 5 Related Work

Several authors have raised the question about quality of metrics used for security assessment [7, 21, 22]. Most of the requirements are empirical and may be considered as good practice. For example, Vaughn et al., [21] state that metrics should clearly characterise the scope of measurement, be sound, have repeatable, reproducible and relevant process of measurement. Andy Ju An Wang [22] adapted four axioms for complexity of programs for security metrics. These axioms looks to be too simple (e.g., "the measure must not assign the same number to all systems") or unclear in the context of security (e.g., "the measure must be sensitive to the ordering of the system components").

We have already shown that our work is close to the analysis of a system with attack graphs. First, both approaches are based on the idea to model behaviour of an attacker as transitions from one state to another. Second, both approaches allow formal description of the model. Third, different metrics can be specified using both approaches: probability of successful attack [23], minimal cost of attack [19], minimal cost of reduction [24], shortest path [18]. Nevertheless, we have a different goal – to formally *analyse* security metrics and check whether they are able to indicate security strength correctly.

There are some metrics defined in a formal way. For example, different versions of an attack surface metric [13, 14, 16] are defined formally. Note, that we had to make some assumptions to model it, e.g., we had to limit amount of

possible attack goals to any attacks on channel, methods, or data (see [10] for details). Another example of formally defined metrics is a "mean time to security failure" metric proposed by Madan et al. [12]. The proposed model considers a single-step attack and its possible effect on the system. In our work we provide a model which is able to capture most of the general security metrics at ones.

Several authors also analysed security of a system taking possible actions of a defender into account [11]. They model system as a graph and consider how attacker propagates towards her goal, and the defender is acting to prevent this to happen. The main difference of such work with our is that we do not consider defender as another active player. We consider defensive actions as modifications of the system in such a way as to enhance security of the system. Thus, in this perspective our work is closer to search for proper cuts in an attack graph [8].

## 6 Conclusions

In this paper, we extended our formal model for analysis of quantitative security metrics. We introduced defensive actions in such a way, that they can only increase the security strength. Then, we analysed security metrics defined in our previous papers [9, 10] in order to check whether the metrics are able to detect the changes of security correctly correctly. The analysis showed that all considered metrics are capable to detect these changes. As a future work, we would like to look for other evident criteria for defining empirical "more secure" relation for a more fine-grained analysis.

## References


1. C. Demetrescu, D. Eppstein, Z. Galil, and G. F. Italiano. Algorithms and theory of computation handbook. In M. J. Atallah and M. Blanton, editors, *Algorithms and theory of computation handbook*, volume 2, chapter Dynamic graph algorithms, pages 9–9. Chapman & Hall/CRC, 2010.
2. L. Finkelstein and M. S. Leaning. A review of the fundamental concepts of measurement. *Measurement*, 2(1):25–34, January-March 1984.
3. D. S. Herrmann. *Complete Guide to Security and Privacy Metrics. Measuring Regulatory Compliance, Operational Resilience, and ROI.* Auerbach Publications, 2007.
4. M. Howard. Fending off future attacks by reducing attack surface, February 2003. available via `http://msdn.microsoft.com/en-us/library/ms972812.aspx`.
5. International Organization for Standardization (ISO). *ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management*, 2005.
6. W. Jansen. Directions in security metric research. Technical Report NISTIR 7564, National institute of Standards and Technology, 2009. available via `http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf` on 28/04/2010.
7. A. Jaquith. *Security metrics: replacing fear, uncertainty, and doubt.* Addison-Wesley, 2007.

8. S. Jha, O. Sheyner, and J. M. Wing. Minimization and reliability analyses of attack graphs. Technical Report CMU-CS-02-109, Carnegie Mellon University, 2002.
9. L. Krautsevich, F. Martinelli, and A. Yautsiukhin. Formal approach to security metrics: what does "more secure" mean for you? In *Proceedings of 4th European Conference on Software Architecture: Companion Volume*, pages 162–169. ACM, 2010.
10. L. Krautsevich, F. Martinelli, and A. Yautsiukhin. Formal analysis of security metrics and risk. In *Proceedings of 5th Workshop on Information Security Theory and Practice of Mobile Devices in Wireless Communication*, pages 304–319. Springer, 2011.
11. K.-W. Lye and J. M. Wing. Game strategies in network security. *International Journal on Information Security*, 4:71–86, 2005.
12. B. B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, and K. S. Trivedi. A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance evaluatin journal*, 1-4(56):167–186, 2004.
13. P. Manadhata and J. Wing. Measuring a system's attack surface. Technical Report CMU-TR-04-102, Carnegie Mellon University, 2004.
14. P. Manadhata and J. M. Wing. An attack surface metric. Technical Report CMU-CS-05-155, School of Computer Science. Carnegie Mellon University, 2005.
15. P. K. Manadhata, D. K. Kaynar, and J. M. Wing. A formal model for a system's attack surface. Technical Report CMU-CS-07-144, Carnegie Mellon University, July 2007.
16. P. K. Manadhata, K. M. C. Tan, R. A. Maxion, and J. M. Wing. An approach to measuring a systems attack surface. Technical Report CMU-CS-07-146, School of Computer Science. Carnegie Mellon University, 2007.
17. F. Martinelli. Analysis of security protocols as open systems. *Theoretical Computer Science*, 290(1):1057–1106, 2003.
18. R. Ortalo, Y. Deswarte, and M. Kaâniche. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Transactions on Software Engineering*, 25(5):633–650, 1999.
19. J. Pamula, S. Jajodia, P. Ammann, and V. Swarup. A weakest-adversary security metric for network configuration security analysis. In *Proceedings of the 2nd ACM Workshop on Quality of Protection*, 2006.
20. P. Suppes and J. L. Zinnes. Basic measurement theory. Technical Report 45, Institute for mathematical studies in the social science, March 1962.
21. R. B. Vaughn, R. Henning, and A. Siraj. Information assurance measures and metrics - state of practice and proposed taxonomy. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences*, January 2003.
22. A. J. A. Wang. Information security models and metrics. In *Proceedings of the 43th Annual Southeast Regional Conference*, pages 178–184, New York, NY, USA, 2005. ACM.
23. L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia. An attack graph-based probabilistic security metric. In *Proceeedings of the 22nd annual IFIP WG 11.3 working conference on Data and Applications Security*, pages 283–296, Berlin, Heidelberg, 2008. Springer-Verlag.
24. L. Wang, S. Noel, and S. Jajodia. Minimum-cost network hardening using attack graphs. *Computer Communications*, 29(18):3812–3824, 2006.