Formal Analysis of Security Metrics with Defensive Actions

Leanid Krautsevich, Fabio Martinelli, and Artsiom Yautsiukhin
Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche
Via G. Moruzzi 1, Pisa 56124, Italy
Email: {firstname.lastname}@iit.cnr.it

***Abstract*—Security management requires quantitative security metrics in order to effectively distribute limited resources and justify investments into security. The problem is not only to select the right security metrics but also to be sure that the selected 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 on interactions between an attacker and a system. We use this model in order to define security metrics and defensive actions which supposed to improve security strength of a system. We exploit these definitions to analyse whether security metrics are able to indicate security improvements correctly.

Keywords*—*Security metrics, defensive actions, attacker, countermeasures.

I. Introduction

Security metrics attract the attention of the security community for more that twenty years [5], [9]. However, the field is still missing a general formal model which is capable of describing security metrics [8]. 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 the first steps towards a model that allows formal definition and analysis of quantitative security metrics, e.g., the number of attacks existing for a system [12], [13]. In our model, we exploited findings of the measurement theory which defines the conditions (known as the representation theorem) which formally state when a metric may be considered as a proper indicator for some quality of an object [3], [23]. We showed that in order to apply the findings of the measurement theory to security metrics we must define an empirical "more secure" relation for systems and only then we are able to check whether a metric correctly represents security of a system. We also made a simple, but evident, assumption that a system with a wider set of possible attacks than another system is less secure. This assumption allowed us to partially check whether the formalised metrics correctly represent the relation between two systems in terms of security strength. The assumption we have made limited our analysis, since we were able to check representativeness only for a limited number of systems.

In this paper, we formally define defensive actions, i.e., the actions which improve security of a system. The defined actions are theoretical in their nature because they have only positive effect on security. On the other hand, this theoretical view allows us to make a new assumption, which defines "more secure" relation for a wider range of systems than the one used in [12]. Using this assumption we check whether the security metrics found in the literature [5], [9], [18], [19], [21], [22], [26] are able to show that the security of the system has been improved. We also show that some real security countermeasures applied by a system administrator or security team may be modelled with these defensive actions.

A. Contributions

The main contributions of this paper are:

- we formally define theoretical defensive actions;
- we provide a new definition of "more secure" relation based on defensive actions;
- we analyse existing security metrics against the newly defined "more secure" relation.

The rest of the paper goes as follows. Section II recalls the details of our basic formal model from [12], [13]. Section III presents the definitions of several general security metrics from our previous work. Section IV introduces the elementary defensive actions and analyses their impact on the values of security metrics. Section V generalises the elementary defensive actions to complex defensive actions, shows the effect on this generalisation on security metrics. Section VI discusses the link between defensive actions and real security countermeasures. Section VII describes the related work. The conclusion is presented in Section VIII.

II. Formal Model

We recall important peculiarities of our formal model [12], [13] 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 [20] and define a perfect security.

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''). We denote a trace of actions accomplished by the system as γ_S and by the attacker as γ_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:

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

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 is preserved. We understand security as a complex concept, i.e., as a preservation of availability, confidentiality, and integrity [7]. 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: $\gamma = a_1 \circ a_2 \circ \ldots \circ a_n$. 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 γ.

Definition 2: An attack to a system S is a trace of actions γ_X:

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

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). We distinguish between an attack and an attempt of attack. An attack is a sequence of actions required to compromise a system. An attempt of attack is a single execution of actions in order to compromise the system.

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 the system S is:

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

We derive a definition that determines the "more secure" relation on the basis of attack sets.

Definition 4: Let $\Gamma_X(S_1)$ be a set of attacks relevant to a system S_1 and $\Gamma_X(S_2)$ 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 ($S_1 \succeq^s_{sec} S_2$) if a set of attacks $\Gamma_X(S_1)$ relevant to the system S_1 is included into a set of attacks $\Gamma_X(S_2)$ relevant to the system S_2 ($\Gamma_X(S_1) \subseteq \Gamma_X(S_2)$):

$$S_1 \succeq^s_{sec} S_2 \Longleftrightarrow \Gamma_X(S_1) \subseteq \Gamma_X(S_2) \quad (4)$$

The "more secure" relation as presented in Definition 4 can be applied only to a limited amount of systems because it is a rare case when attacks to one system are completely included into an attack set of another system. More sophisticated criteria are required for a precise definition of a general "more secure" relation $\succeq_{sec}$. While such criteria are currently absent, we assume that our definition of simple "more secure" relation on the basis of attacks sets could give the same order of the systems as a general relation if the simple relation is applicable. In other words, we make the following assumption.

Assumption 1:

$$\succeq^s_{sec} \quad \subseteq \quad \succeq_{sec} \quad (5)$$

Formally a relation (e.g., $\succeq^s_{sec}$) is the set of ordered pairs of elements [4]. Thus, the set of systems compared on the basis of the relation $\succeq^s_{sec}$ is the subset of systems compared using the relation $\succeq_{sec}$.

In other words, we assume that the relation we have defined is the same as the general relation, but is applicable only for specific pairs of systems, i.e., the simple relation gives only partial order over a set $\mathbb{S}$ of systems.

III. Definitions of Metrics

We exploit the formal model to define several general quantitative security metrics. Moreover, for each metric we introduce the representation theorem which is defined in measurement theory for the correct assessment of an empirical system. Metrics must satisfy the representation theorem [3], [23]. For our case the theorem is seen as follows.

Theorem 1: Let S_1 and S_2 be two systems from a set of systems $\mathbb{S}$ and $\mathscr{M} : \mathbb{S} \mapsto \mathbb{R}$ be an objective-empirical function which assigns a real value to an element from $\mathbb{S}$. Then:

$$S_1 \succeq_{sec} S_2 \Longleftrightarrow \mathscr{M}(S_1) \succeq_{\mathscr{M}} \mathscr{M}(S_2) \quad (6)$$

Where $\mathscr{M}(S)$ denotes that the metric $\mathscr{M}$ is computed for a system S (e.g., for a workstation with all hardware and software installed), $\mathscr{M}(S_1) \succeq_{\mathscr{M}} \mathscr{M}(S_2)$ means than $\mathscr{M}(S_1)$ 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).

Usually the security metrics are introduced in such a way that they satisfy the representation theorem by definition, thus, better metrics values mean better security and systems with better security have better metrics values. We provide formal definitions for several quantitative security metrics.

1) 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 on a system exist the less secure the system is. This metric is applied for the simplest analysis of attack graphs [21], [22]. Number of attacks also can be used for the analysis of results of the penetration testing.

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

$$N_{att}(S) = |\Gamma_X(S)| \quad (7)$$

Representation theorem for the number of attacks:

$$S_1 \succeq_{sec} S_2 \Longleftrightarrow N_{att}(S_1) \leq N_{att}(S_2) \quad (8)$$

2) Minimal cost of attack: Minimal cost of attack represents the minimal cost that the attacker has to pay for the execution of an attack on a system [22].

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

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

$$C(\gamma_X) = \sum_{\forall a \in \gamma_X} C(a), \gamma_X = a_1 \circ a_2 \circ \cdots \circ a_n \tag{9}$$

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

$$C^{min}(S) = \min_{\forall \gamma_X \in \Gamma_X(S)} \{C(\gamma_X) : \gamma_X \in \Gamma_X(S)\} \tag{10}$$

Representation theorem for the minimal cost of attack:

$$S_1 \succeq_{sec} S_2 \Longleftrightarrow C^{min}(S_1) \geq C^{min}(S_2) \tag{11}$$

3) Minimal 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 [21]. We start with the definition of an attack length:

Definition 8: The length $L(\gamma_X)$ of attack γ_X is:

$$L(\gamma_X) = |\gamma_X| \tag{12}$$

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

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

$$L^{min}(S) = \min_{\forall \gamma_X \in \Gamma_X(S)} \{L(\gamma_X) : \gamma_X \in \Gamma_X(S)\} \tag{13}$$

Representation theorem for the minimal length of attack:

$$S_1 \succeq_{sec} S_2 \Longleftrightarrow L^{min}(S_1) \geq L^{min}(S_2) \tag{14}$$

4) Maximal probability of successful attack: The probability to accomplish an attack successfully is a well-known metric [26]. The metric describes the most probable way to compromise the system.

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

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

$$\mathbf{Pr}(\gamma_X) = \prod_{\forall a \in \gamma_X} \mathbf{Pr}(a), \gamma_X = a_1 \circ a_2 \circ \cdots \circ a_n \tag{15}$$

We assumed that the successful executions of attack actions are independent.

Definition 11: We define maximal probability of successful attack $\mathbf{Pr}^{max}(S)$ as:

$$\mathbf{Pr}^{max}(S) = \max_{\forall \gamma_X \in X} \{\mathbf{Pr}(\gamma_X) : \gamma_X \in \Gamma_X(S)\} \tag{16}$$

Representative theorem for the maximal probability of attack:

$$S_1 \succeq_{sec} S_2 \Longleftrightarrow \mathbf{Pr}^{max}(S_1) \leq \mathbf{Pr}^{max}(S_2) \tag{17}$$

5) Attack surface metric: This metric has been proposed by Howard [6] and Manadhata and Wing [16]. Here we consider one of the latest versions of attack surface metric presented by Manadhata et al. [18], [19].

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 reached after successful execution of attach γ_X. Let us also know the level of privileges required for successful execution of an action a, denoted as $priv(a)$. The level of privileges $priv(a)$ can be seen as a non-negative natural value [19]. Thus, the level of privileges gained executing a sequence of actions is:

$$priv(\gamma_X) = \max_{\forall a \in \gamma_X} \{priv(a), \gamma_X \in \Gamma_X(S)\} \tag{18}$$

For every system we can assign the following tuple:

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

Here:

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

$$Risk^c = \sum_{\forall \gamma_X \in \Gamma^c} \frac{dmg_{pot}(\gamma_X)}{priv(\gamma_X)}$$

$$Risk^d = \sum_{\forall \gamma_X \in \Gamma^d} \frac{dmg_{pot}(\gamma_X)}{priv(\gamma_X)}$$

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

Representative theorem for the attack surface:

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

While authors of metrics *assume* that the metrics satisfy representation theorem, the measurements theory *requires a formal proof* of the satisfaction. The issue of the formal proof comes from the point discussed in Section II. There is no widely accepted definition of the general "more secure" relation. Thus, it is impossible to check whether metrics satisfy the theorem until the general relation is not defined. In our earlier work [12], we tried to overcome the issue analysing the metrics versus the simple "more secure" relation presented in Definition 4. For each metric described above we proved theorems of the following form.

Theorem 2:

$$\Gamma_X(S_1) \subseteq \Gamma_X(S_2) \Longrightarrow \mathscr{M}(S_1) \succeq_{\mathscr{M}} \mathscr{M}(S_2) \tag{22}$$

This theorem is a simplified version of the following statement derived from Definition 4, Assumption 1, and Theorem 1:

$$\Gamma_X(S_1) \subseteq \Gamma_X(S_2) \Longleftrightarrow S_1 \succeq^s_{sec} S_2 \Longrightarrow \\ S_1 \succeq_{sec} S_2 \Longleftrightarrow \mathscr{M}(S_1) \succeq_{\mathscr{M}} \mathscr{M}(S_2) \tag{23}$$

This theorem cannot be seen as a complete substitution of Theorem 1, but allowed us to perform partial analysis since general "more secure" relation is unknown. Next in this paper, we try to define another "more secure" relation which allows comparing more pairs of systems.

IV. Elementary Defensive Actions

A 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. We would like to consider an idealistic case when all modifications are applied correctly, i.e., no additional threats (i.e., additional actions) are added. We also consider only such modifications, which do not conflict with each other. In order to model such changes of the system, we first define elementary defensive actions similar to the ones specified for graphs [2]: insert action, delete action, and change label. We would like to note that defensive actions and ordinary actions of our model have different nature and, thus, 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, and do not consider the current state of the process.

Definition 13: Let $S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X}$ 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 elementary defensive actions $D_{smpl} = \{d^{del}, d^{ins}, d^{sub}\}$.

1) An elementary defensive action $d^{del} \in D_{smpl}$ deletes an action a (and does not change other actions):

$$\begin{aligned} &\exists a, \exists \gamma \ . \ \gamma = \gamma_1 \circ a \circ \gamma_2 = \gamma_S \bullet \gamma_X, \\ &\gamma_X \in \Gamma_X(S) \ . \ S' \xrightarrow{a} S'' \ (or \ X' \xrightarrow{a} X''), \\ &\nexists \hat{\gamma} \ . \ a \in \hat{\gamma} = \gamma_1 \circ a \circ \gamma_2 = \hat{\gamma}_S \bullet \hat{\gamma}_X, \\ &\hat{\gamma}_X \in \Gamma_X(\hat{S}) \ . \ \hat{S}' \xrightarrow{a} \hat{S}'' \ (or \ \hat{X}' \xrightarrow{a} \hat{X}''), \\ &\forall a' \neq a, S''' \xrightarrow{a'} S'''' \wedge \hat{S}''' \xrightarrow{a'} \hat{S}'''' \\ &(or \ X''' \xrightarrow{a'} X'''' \wedge \hat{X}''' \xrightarrow{a'} \hat{X}'''') \end{aligned} \tag{24}$$

Lines 1-2 state that we focus on one specific action which belongs to a trace which leads an attacker to its goal. Lines 3-4 state that there is no such action in the modified system any more, i.e., the attacker is not able to execute this attack. Lines 5-6 state that any other actions but the one we considered are left in both systems.

2) An elementary defensive action $d^{ins} \in D_{smpl}$ inserts an action $\hat{a}$ in the middle of an existing attack (and does not change other actions):

$$\begin{aligned} &\exists \hat{a}, \exists \hat{\gamma} \ . \ \hat{\gamma} = \gamma_1 \circ \hat{a} \circ \gamma_2 = \hat{\gamma}_S \bullet \hat{\gamma}_X, \\ &\hat{\gamma}_X \in \Gamma_X(\hat{S}) \ . \ \hat{S}' \xrightarrow{\hat{a}} \hat{S}'' \ (or \ \hat{X}' \xrightarrow{\hat{a}} \hat{X}''), \\ &\exists \gamma, \hat{a} \notin \gamma = \gamma_1 \circ \gamma_2 = \gamma_S \bullet \gamma_X, \\ &\gamma_X \in \Gamma_X(S) \ . \ S' \xrightarrow{\hat{a}} S'' \ (or \ X' \xrightarrow{\hat{a}} X''), \\ &\forall a' \neq \hat{a}, S''' \xrightarrow{a'} S'''' \wedge \hat{S}''' \xrightarrow{a'} \hat{S}'''' \\ &(or \ X''' \xrightarrow{a'} X'''' \wedge \hat{X}''' \xrightarrow{a'} \hat{X}'''') \end{aligned} \tag{25}$$

Lines 1-2 state that we add a new action in one trace of actions of the changed system. Line 3-4 say that the considered action did not belong to the system before the change. Lines 5-6 state that no other changes apart of inserting an action have been performed.

3) An elementary defensive action $d^{sub} \in D_{smpl}$ substitutes (re-labels) an action a with a better from the security point of view action $\hat{a}$ (and does not change other actions):

$$\begin{aligned} &\exists a, \exists \gamma \ . \ \gamma = \gamma_1 \circ a \circ \gamma_2 = \gamma_S \bullet \gamma_X, \\ &\gamma_X \in \Gamma_X(S) \ . \ S' \xrightarrow{a} S'' \ (or \ X' \xrightarrow{a} X''), \\ &\exists \hat{a}, \exists \hat{\gamma} \ . \ a \notin \hat{\gamma}, \\ &\hat{a} \in \hat{\gamma} = \gamma_1 \circ \hat{a} \circ \gamma_2 = \hat{\gamma}_S \bullet \hat{\gamma}_X, \\ &\hat{\gamma}_X \in \Gamma_X(\hat{S}) \ . \ \hat{S}' \xrightarrow{\hat{a}} \hat{S}'' \ (or \ \hat{X}' \xrightarrow{\hat{a}} \hat{X}''), \\ &\forall lb \ . \ lb(\hat{a}) \succeq_{\mathscr{M}} lb(a), \\ &\forall a' \ . \ a' \neq a, a' \neq \hat{a}, \\ &S''' \xrightarrow{a'} S'''' \wedge \hat{S}''' \xrightarrow{a'} \hat{S}'''' \\ &(or \ X''' \xrightarrow{a'} X'''' \wedge \hat{X}''' \xrightarrow{a'} \hat{X}'''') \end{aligned} \tag{26}$$

Lines 1-5 say that we remove one action and add a new action into the position of the deleted action. The sixth line states that the new action has all labels better or equal from the security point of view than the one we had before the change. The last three lines assure that other actions are not changed. Note, that we can see this action as simple re-labelling, i.e., improving the label of an action from security point of view.

In Definition 13, we considered processes with hats (e.g., $\hat{S}$) as the same processes without hats (e.g, S) but the ones we have after applying a defensive action. Although, we acknowledge that some defensive actions may affect only a system, when others affect only an attacker, we mark both processes changed for brevity. Thus, in some cases one of the processes could be the same (e.g., if we remove an action of a system, an attacker could be the same $X = \hat{X}$).

Property 1: Applying the simplest defensive actions does not increase the number of attacks to the system:

$$\begin{aligned} \forall d \in D_{smpl} \ \forall S, X \ . \ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \\ |\Gamma_X(S)| \geq |\Gamma_X(\hat{S})| \end{aligned} \tag{27}$$

Proof: Definition of every elementary defensive action includes a statement which states that only one trace of action is affected. This means that all attacks, but the affected one, are the same for both systems. Thus, let Δ_X be a set of affected attacks in the system before the change, while $\hat{\Delta}_X$ be a set of affected attacks in the system after the change. Since, only one attack may be affected then both sets may include only one element or be empty. If E/E' denotes the exclusion of elements of a set E' from a set of elements E (subtraction of sets), then we can state, that $\Gamma_X(S)/\Delta_X = \Gamma_X(\hat{S})/\hat{\Delta}_X$. Thus, we focus only on the changed part.

1) **Delete an action a.** The first two lines in Equation 24 state that the deleted action belongs to a sequence γ which leads to a compromised state and includes an attack $\gamma = \gamma_S \bullet \gamma_X, \gamma_X \in \Gamma_X(S)$. The deletion of action makes the sequence γ no longer executable

to reach a compromised state (i.e., $\hat{\Delta}_X = \emptyset$, while $\Delta_X = \{\gamma_X\}$). Thus:

$$|\Gamma_X(S)| = |\Gamma_X(S)/\Delta_X| + |\Delta_X|,$$
$$|\Gamma_X(\hat{S})| = |\Gamma_X(\hat{S})/\hat{\Delta}_X| + |\hat{\Delta}_X| \Longrightarrow$$
$$|\Gamma_X(S)| > |\Gamma_X(\hat{S})|$$

2) **Insert an action $\hat{a}$.** Equation 25 states that the old version of the system S has a sequence $\gamma = \gamma_1 \circ \gamma_2$ which makes an attack possible (line 3), while the new one has a different trace $\hat{\gamma} = \gamma_1 \circ \hat{a} \circ \gamma_2$ (line 1) instead. Line 5 assures that no other attacks neither in the old nor in the new versions are affected. I.e., $\hat{\Delta}_X = \{\hat{\gamma}_X\}$ and $\Delta_X = \{\gamma_X\}$. Thus:

$$|\Gamma_X(S)| = |\Gamma_X(S)/\Delta_X| + |\Delta_X|,$$
$$|\Gamma_X(\hat{S})| = |\Gamma_X(\hat{S})/\hat{\Delta}_X| + |\hat{\Delta}_X| \Longrightarrow$$
$$|\Gamma_X(S)| = |\Gamma_X(\hat{S})|$$

3) **Substitute an action a with action $\hat{a}$.** This means that for a sequence $\gamma = \gamma_S \bullet \gamma_X = \gamma_1 \circ a \circ \gamma_2, \gamma_X \in \Gamma_X(S)$ there is a sequence $\hat{\gamma} = \hat{\gamma}_S \bullet \hat{\gamma}_X = \gamma_1 \circ \hat{a} \circ \gamma_2, \hat{\gamma}_X \in \Gamma_X(\hat{S})$. I.e., $\hat{\Delta}_X = \{\hat{\gamma}_X\}$ and $\Delta_X = \{\gamma_X\}$. Thus:

$$|\Gamma_X(S)| = |\Gamma_X(S)/\Delta_X| + |\Delta_X|,$$
$$|\Gamma_X(\hat{S})| = |\Gamma_X(\hat{S})/\hat{\Delta}_X| + |\hat{\Delta}_X| \Longrightarrow$$
$$|\Gamma_X(S)| = |\Gamma_X(\hat{S})|$$

■

A. Analysis of Effect of Elementary Defensive Actions on Metrics

The defensive actions aim at making a system more secure. We propose a new definition based on elementary defensive actions which is similar to Definition 4:

Definition 14:

$$\forall d \in D_{smpl}\ \forall S, X\ .\ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longleftrightarrow \hat{S} \succeq^{e}_{sec} S \quad (28)$$

We assume that the relation $\succeq^{e}_{sec}$ is still a part of the general "more secure" relation $\succeq_{sec}$:

Assumption 2:

$$\succeq^{e}_{sec} \quad \subseteq \quad \succeq_{sec} \quad (29)$$

We would like to check whether the security metrics are compatible with Definition 14, i.e., capture effects of the elementary defensive actions. In our earlier work [12], we showed that removing an action is detected by the metrics. Thus, focus only on the elementary defensive action d^{ins} and d^{sub} in the following theorems.

Theorem 3: For number of attacks:

$$\forall d \in D_{smpl}\ \forall S, X\ .\ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \quad (30)$$
$$N_{att}(\hat{S}) \leq N_{att}(S)$$

Proof:

$$N_{att}(S) = |\Gamma_X(S)|, N_{att}(\hat{S}) = |\Gamma_X(\hat{S})|$$

From Property 1:

$$|\Gamma_X(\hat{S})| \leq |\Gamma_X(S)| \Longrightarrow N_{att}(\hat{S}) \leq N_{att}(S)$$

■

Theorem 4: For minimal cost of attack:

$$\forall d \in D_{smpl}\ \forall S, X\ .\ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \quad (31)$$
$$C^{min}_{att}(S) \leq C^{min}_{att}(\hat{S})$$

Proof: It is not necessary that the attack with the minimal cost is impacted by the defensive action. Generally any existing attack may be impacted by the action. A new longer sequence of actions $\hat{\gamma} = \hat{\gamma}_X \bullet \hat{\gamma}_S$ appears instead of a sequence γ due to a insertion of an action $\hat{a}$. The action may belong to $\hat{\gamma}_X$ or to $\hat{\gamma}_S$. In the first case, the cost of the attack increases or stays the same:

$$C(\hat{\gamma}_X) = C(\gamma_X) + C(\hat{a}), C(\hat{a}) \geq 0 \Longrightarrow$$
$$C(\hat{\gamma}_X) \geq C(\gamma_X)$$

In the second case, the cost of the attack is the same as before changes:

$$C(\hat{\gamma}_X) = C(\gamma_X)$$

Substitution of an action changes the label of an action to a label with a better value from the security point of view $lb(\hat{a}) \succeq_{\mathscr{M}} lb(a)$. This means that $C(\hat{a}) \geq C(a)$, i.e., it is more costly for the attacker to execute the new action rather than the old one. Since $\hat{\gamma} = \hat{\gamma}_S \bullet \hat{\gamma}_X$ then either:

$$\hat{a} \in \hat{\gamma}_S, C(\hat{\gamma}_X) = C(\gamma_X)$$

or:

$$\hat{a} \in \hat{\gamma}_X, C(\hat{\gamma}_X) = C(\gamma_X) - C(a) + C(\hat{a}) \Longrightarrow$$
$$C(\hat{\gamma}_X) \geq C(\gamma_X)$$

Thus, for any attack impacted by the defensive action $C(\hat{\gamma}_X) \geq C(\gamma_X)$. Minimal cost of attack in any case is:

$$C^{min}(\hat{S}) \geq C^{min}(S)$$

■

Theorem 5: For minimal length of attack:

$$\forall d \in D_{smpl}\ \forall S, X\ .\ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \quad (32)$$
$$L^{min}(\hat{S}) \geq L^{min}(S)$$

$$\forall d \in D_{smpl}\ \forall S, X\ .\ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \quad (33)$$
$$L^{min}(\hat{S}) \geq L^{min}(S)$$

Proof: The insertion of an action simply increases the length of a single attack (and only it). If the added action:

$$\hat{a} \in \hat{\gamma}_X, L(\gamma_X) = |\gamma_X|, L(\hat{\gamma}_X) = |\hat{\gamma}_X| = |\gamma_X| + 1 \Longrightarrow$$
$$L(\hat{\gamma}_X) > L(\gamma_X)$$

and if:

$$\hat{a} \in \hat{\gamma}_S, L(\gamma_X) = |\gamma_X|, L(\hat{\gamma}_X) = |\hat{\gamma}_X| \Longrightarrow$$
$$L(\hat{\gamma}_X) = L(\gamma_X)$$

The substitution of an action does not change the length of the considered attack:

$$L(\hat{\gamma}_X) = L(\gamma_X)$$

Therefore both for insertion of action and substitution of action $L(\hat{\gamma}_X) \geq L(\gamma_X)$ for any impacted attack. In particular, for the attack with minimal length:

$$L^{min}(\hat{S}) \geq L^{min}(S)$$

■

Theorem 6: For maximal probability of attack:

$$\forall d \in D_{smpl}\ \forall S, X\ .\ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \mathbf{Pr}^{max}(\hat{S}) \leq \mathbf{Pr}^{max}(S) \tag{34}$$

Proof: Using the same reasoning applied to the proof of minimal cost, we can show that $\mathbf{Pr}(\hat{\gamma}_X) \leq \mathbf{Pr}(\gamma_X)$ and $\mathbf{Pr}^{max}(\hat{S}) \leq \mathbf{Pr}^{max}(S)$. ■

Theorem 7: For attack surface:

$$\forall d \in D_{smpl}\ \forall S, X\ .\ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow ASM(\hat{S}) \leq ASM(S) \tag{35}$$

Proof: First of all, since we compare systems out of the context, then we should make equal conditions for two compared systems. Thus, we assume, that $dmg_{pot}(\gamma_X)$ has the same value in both systems, i.e., the achieved utility for the attacker is the same in case of successful execution of the sequence γ_X of actions.

In our previous work [12] we considered an old version of attack surface metric. Since in this paper we use the new version of the metric, we also need to prove the proposition for the first elementary defensive action, i.e., delete an action a. Deleting an action causes removing a single attack to the system:

$$\Gamma_X(\hat{S}) \subset \Gamma_X(S)$$

Smaller number of attacks means smaller number of non-negative summands for $Risk^m$, $Risk^c$, or $Risk^d$ (Definition 12 and [13]) therefore the value of some of these risks reduces and the attack surface also reduces:

$$ASM(\hat{S}) < ASM(S)$$

The insertion of an action $\hat{a}$ increases or leaves the same the required level of privileges for an attack if:

$$\hat{a} \in \hat{\gamma}_X, priv(\hat{\gamma}_X) \geq priv(\gamma_X)$$

and does not change it if:

$$\hat{a} \in \hat{\gamma}_S, priv(\hat{\gamma}_X) = priv(\gamma_X)$$

Thus, the summands contributing the attack surface decrease and the attack surface decreases as well.

Substituting an action in a way that $lb(\hat{a}) \succeq_{\mathscr{M}} lb(a)$ also increases or lefts the same required privileges for execution of an attack $priv(\hat{a}) \geq priv(a)$:

$$\hat{a} \in \hat{\gamma}_X, priv(\hat{\gamma}_X) \geq priv(\gamma_X)$$
$$\hat{a} \in \hat{\gamma}_S, priv(\hat{\gamma}_X) = priv(\gamma_X)$$

which leads to decrease of the attack surface.

Thus, for each elementary defensive action the attack surface decreases or stays the same:

$$ASM(\hat{S}) \leq ASM(S)$$

■

We have shown that all metrics are able to correctly indicate the elementary defensive actions applied to a system.

V. Complex Defensive Actions

Elementary defensive actions can be combined into complex defensive actions. We would like to analyse whether application of complex defensive actions to a system is still correctly captured by the security metrics. To do this, we define complex defensive actions as a sequence of elementary defensive actions.

Definition 15: Let $d_1, d_2, \ldots, d_n \in D_{smpl}$ then a complex defensive action β is: $\beta = d_1 \circ d_2 \circ \ldots \circ d_n\ .\ S||X \stackrel{d_1}{\Rightarrow} S_1||X_1 \stackrel{d_2}{\Rightarrow} \ldots \stackrel{d_n}{\Rightarrow} \hat{S}||\hat{X}$ which denotes that complex defensive action β is applied action by action and now processes S and X are changed to $\hat{S}$ and $\hat{X}$.

We define another security relation to show that an application of a complex defensive action makes a system more secure.

Definition 16:

$$\forall \beta\ \forall S, X\ .\ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X} \Longleftrightarrow \hat{S} \succeq^c_{sec} S \tag{36}$$

We formally show the transitivity of the relation.

Property 2:

$$S_1 \succeq^c_{sec} S_2, S_2 \succeq^c_{sec} S_3 \Longrightarrow S_1 \succeq^c_{sec} S_3$$

Proof: By the Definitions 15 and 16:

$$\exists \beta_1, \beta_2\ .\ S_3||X_3 \stackrel{\beta_1}{\Rightarrow} S_2||X_2, S_2||X_2 \stackrel{\beta_2}{\Rightarrow} S_1||X_1$$

Since $\beta_3 = \beta_1 \circ \beta_2$ is also a complex defensive action, then by Definition 15 $S_3||X_3 \stackrel{\beta_3}{\Rightarrow} S_1||X_1$ and by Definition 16 $S_1 \succeq^c_{sec} S_3$. ■

Again we assume that the relation $\succeq^c_{sec}$ is a part of the general "more secure" relation $\succeq_{sec}$.

Assumption 3:

$$\succeq^c_{sec} \ \subset \ \succeq_{sec} \tag{37}$$

We analyse the connection between the newly defined relation $\succeq^c_{sec}$ and the relations $\succeq^s_{sec}$ ans $\succeq^e_{sec}$. The simple "more secure" relation $\succeq^s_{sec}$ is the part of the relation $\succeq^c_{sec}$.

Property 3:

$$\succeq^s_{sec} \ \subset \ \succeq^c_{sec} \tag{38}$$

Proof: Definitions 4 and 16 shows that we should prove:

$$\forall \hat{S}, S\ .\ \Gamma_X(\hat{S}) \subseteq \Gamma_X(S) \Longrightarrow \exists \beta\ .\ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X}$$

Let $\Gamma_X(S) = \Gamma_X(\hat{S}) \cup \Delta_X$. For every $\gamma_X^i \in \Delta_X$ we can find d_i^{del}, which eliminates this attack according to Definition 13.1. We can compose a complex defensive action β according to Definition 15 as:

$$\exists \beta = d_1^{del} \circ d_2^{del} \circ \ldots \circ d_n^{del} \ . \ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X}$$

■

The "more secure" relation $\succeq_{sec}^{e}$ defined on the basis of elementary defensive actions is the part of the relation $\succeq_{sec}^{c}$ defined on the basis of complex defensive actions.

Property 4:

$$\succeq_{sec}^{e} \quad \subset \quad \succeq_{sec}^{c} \tag{39}$$

Proof: Definitions 14 and 16 shows that we should prove:

$$\forall d \in D \ \forall S, X \ . \ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \exists \beta \ . \ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X}$$

This trivially follows from Definition 15 of complex defensive action when $\beta = d$, i.e., for the complex defensive action consisting of a single elementary defensive action. ■

Thus, Definition 16 is more general than Definition 4 and 14, i.e., it is applicable to a much wider set of systems.

Theorem 8:

$$\begin{aligned}
&\forall \beta \ \forall S, X \ . \ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \\
&\qquad N_{att}(\hat{S}) \leq N_{att}(S) \\
&\forall \beta \ \forall S, X \ . \ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \\
&\qquad C_{att}^{min}(\hat{S}) \geq C_{att}^{min}(S) \\
&\forall \beta \ \forall S, X \ . \ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \\
&\qquad L^{min}(\hat{S}) \geq L^{min}(S) \\
&\forall \beta \ \forall S, X \ . \ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \\
&\qquad \mathbf{Pr}^{max}(\hat{S}) \leq \mathbf{Pr}^{max}(S) \\
&\forall \beta \ \forall S, X \ . \ S||X \stackrel{\beta}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \\
&\qquad ASM(\hat{S}) \leq ASM(S)
\end{aligned} \tag{40}$$

Proof: β can be seen as a sequence of elementary defensive actions by Definition 15. In Section III, we have already proved for all $\mathscr{M}$ that:

$$\forall d \ \forall S, X \ . \ S||X \stackrel{d}{\Rightarrow} \hat{S}||\hat{X} \Longrightarrow \mathscr{M}(\hat{S}) \succeq_{\mathscr{M}} \mathscr{M}(S)$$

Let $\beta = d_1 \circ d_2 \circ \ldots d_n$ then $S||X \stackrel{d_1}{\Rightarrow} S_1||X_1 \stackrel{d_2}{\Rightarrow} \ldots \stackrel{d_n}{\Rightarrow} \hat{S}||\hat{X}$ and for all $\mathscr{M}$: $\mathscr{M}(\hat{S}) \succeq_{\mathscr{M}} \ldots \succeq_{\mathscr{M}} \mathscr{M}(S_1) \succeq_{\mathscr{M}} \mathscr{M}(S)$. Thus, $\mathscr{M}(\hat{S}) \succeq_{\mathscr{M}} \mathscr{M}(S)$ because $\succeq_{\mathscr{M}}$ is a transitive relation since both its numerical instances $\geq$ and $\leq$ are transitive. ■

The final remark here is that the provided analysis is valid not only for a system that is changed by applying only security patches. The analysis is also valid for a system that is changed in a way that the change can be represented using a sequence of elementary defensive actions.

VI. Discussion

We would like to discuss a relation between elementary and complex defensive actions and real security countermeasures applied by system administrators and security teams.

The defensive actions considered in the paper are theoretical and defined (Definitions 13,14 and 15,16 under Assumptions 2 and 3) in a way that they can only improve the security of a system. Such definitions are useful for theoretical analysis of security metrics.

The real security countermeasures can be usually seen as complex defensive actions. Such countermeasures aim at improving security of a system as a whole. Unfortunately, it is not always the case that an installed firewall or a new security policy for an access control system have only positive effect on security. Some security countermeasures may have security flaws, for instance, incorrectly created access control policy may allow access to unwanted users. Moreover, even a well forged countermeasure may have a negative effect on security because additional protection for one security area may allow new attacks in another area, for example, logs may open a new possibility to compromise confidentiality of a system. Therefore, for modelling real security countermeasures it is not enough to consider only the defensive actions described in the paper. Such modelling may be performed in scope of the proposed formal model if the formal model will be extended. However it is not the goal of the current paper.

VII. Related Work

Several authors raised the question about quality of metrics used for security evaluation [9], [24], [25]. Most of the requirements are empirical and may be considered as a good practice. For example, Vaughn et al. [24] stated that metrics should clearly characterise the scope of measurement, be sound, have repeatable, reproducible and relevant process of measurement. Andy Ju An Wang [25] 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").

Our approach 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, different metrics can be specified using both approaches: probability of successful attack [26], minimal cost of attack [22], minimal cost of reduction [27], shortest path [21]. Nevertheless, we have a different goal: to *formally analyse* security metrics and check whether they are able to indicate security strength correctly, while attack graphs serve for the analysis and evaluation of security of systems.

There are several metrics defined using models different than attack graphs. One metric is attack surface [16], [17], [19]. We had to make some assumptions to model it, e.g., we had to limit of possible attacks to only attacks on channels, methods, and data (see [13] for details). Another metric is a mean time to security failure proposed by Madan et al. [15]. The metric 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.

Several authors analysed security of a system taking possible actions of a defender into account [1], [11], [14]. They exploit defence trees and attack graphs 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 one is that we do not consider defender as another active player. We consider defensive actions as modifications of the system in a way that improves security of the system. Thus, in this perspective our work is closer to search for proper cuts in an attack graph [10].

VIII. Conclusions

In this paper, we extended our formal model for analysis of quantitative security metrics [12], [13]. We introduced elementary and complex defensive actions in a way that they can only increase the security strength. Then, we analysed several security metrics in order to check whether the metrics are able to detect the changes of security correctly. The analysis showed that all considered metrics are capable to detect these changes. This means that we have no evidence that these metrics are bad for the evaluation of security. Unfortunately, it is still not enough to say that the metrics are always good for the evaluation of security according to the representativeness theorem because the general "more secure" relation is still absent. However we made another step towards the definition of the general "more secure" relation.

As a future work, we would like to look for other evident criteria for defining "more secure" relation to perform a more fine-grained analysis of security metrics. Another direction may be to extend the model to capture real security countermeasures. Moreover, we can consider a defender as an active entity in our model.

References

[1] S. Bistarelli, M. Dall'Aglio, and P. Peretti. Strategic games on defense trees. In *Proceedings of 4th International Workshop on Formal Aspects in Security and Trust*, pages 1–15. Springer, 2007.

[2] 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.

[3] L. Finkelstein and M. S. Leaning. A review of the fundamental concepts of measurement. *Measurement*, 2(1):25–34, January-March 1984.

[4] J. H. Gallier. *Logic for computer science. Foundations of automatic theorem proving.* University of Pennsylvania, 2003.

[5] D. S. Herrmann. *Complete Guide to Security and Privacy Metrics. Measuring Regulatory Compliance, Operational Resilience, and ROI.* Auerbach Publications, 2007.

[6] M. Howard. Fending off future attacks by reducing attack surface, February 2003. available via http://msdn.microsoft.com/en-us/library/ms972812.aspx.

[7] International Organization for Standardization (ISO). *ISO/IEC 27002:2005 Information technology – Security techniques – Code of practice for information security management*, 2005.

[8] 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.

[9] A. Jaquith. *Security metrics: replacing fear, uncertainty, and doubt*. Addison-Wesley, 2007.

[10] 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.

[11] B. Kordy, S. Mauw, and P. Schweitzer. Quantitative questions on attackdefense trees. In *Proceedings of 15th International Conference on Information Security and Cryptology*, pages 49–64. Springer, 2012.

[12] 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.

[13] 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.

[14] K.-W. Lye and J. M. Wing. Game strategies in network security. *International Journal on Information Security*, 4:71–86, 2005.

[15] 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.

[16] P. Manadhata and J. Wing. Measuring a system's attack surface. Technical Report CMU-TR-04-102, Carnegie Mellon University, 2004.

[17] P. Manadhata and J. M. Wing. An attack surface metric. Technical Report CMU-CS-05-155, School of Computer Science. Carnegie Mellon University, 2005.

[18] 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.

[19] 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.

[20] F. Martinelli. Analysis of security protocols as open systems. *Theoretical Computer Science*, 290(1):1057–1106, 2003.

[21] 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.

[22] 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.

[23] P. Suppes and J. L. Zinnes. Basic measurement theory. Technical Report 45, Institute for mathematical studies in the social science, March 1962.

[24] 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.

[25] 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.

[26] 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.

[27] L. Wang, S. Noel, and S. Jajodia. Minimum-cost network hardening using attack graphs. *Computer Communications*, 29(18):3812–3824, 2006.