Formal Analysis of Security Metrics and Risk

Leanid Krautsevich, Fabio Martinelli, Artsiom Yautsiukhin

Formal Analysis of Security Metrics and Risk*

Leanid Krautsevich[1], Fabio Martinelli[2], and Artsiom Yautsiukhin[2]

[1] Department of Computer Science, University of Pisa, Pisa, Italy
{krautsev}@di.unipi.it
[2] Istituto di Informatica e Telematica, Consiglio Nazionale delle Ricerche, Pisa, Italy
{fabio.martinelli,artsiom.yautsiukhin}@iit.cnr.it

Abstract. Security metrics are usually defined informally and, therefore, the rigourous analysis of these metrics is a hard task. This analysis is required to identify the existing relations between the security metrics, which try to quantify the same quality: security.
Risk, computed as Annualised Loss Expectancy, is often used in order to give the overall assessment of security as a whole. Risk and security metrics are usually defined separately and the relation between these indicators have not been considered thoroughly. In this work we fill this gap by providing a formal definition of risk and formal analysis of relations between security metrics and risk.

1 Introduction

Quantification of security is a problem which has gained much attention recently [7, 10, 24, 25]. The results of such quantification are needed for various purposes. First of all, the classical purpose is to understand how secure the system is and to determine if additional security controls are required [7, 10]. The second purpose is to compare the level of security of a system with others [17, 21]. Nowadays, Service Oriented Architecture becomes more and more popular. Therefore, quantification of security is required for advertisement of a good protection level of a service, for accurate stating the quality of protection level in service level agreements, and for selection of the most suitable and secure services [12, 3, 21].

There are a number of security metrics which are used in order to analyse the strength of security systems [7, 10, 20, 17, 21]. Although these metrics are widely used in security literature none of them (even a finite set of such metrics) can give a complete view of security strength. Moreover, the relations between the metrics, their contribution to the overall level of protection, and sensitivity are unclear. In other words, we do not know which metric is the best approximation of security level. Without this knowledge we appear in a situation when usage of different metrics leads to very different decisions.

Risk analysis is the most widely used method for analysing the complete picture of security state [23, 2, 5]. The main goal of this analysis is to compute

* This work is partially supported by FP7-ICT-2009-5 NESSOS and FP7-ICT-2009-5 ANIKETOS projects.

the amount of possible losses which are caused by occurrences of various threats. Although this technique is not perfect [10, 22], it has many advantages: the technique is general enough to be applied to any system, its results provide the complete vision of security, it helps to justify investments in security, and such justification is understandable for financial managers and general directors.

Currently, security metrics and risk exist apart from each other and the relation between these indicators, although assumed, is not specified. On the other hand, risk is supposed to be one of the most general security indicator. Thus, risk already must incorporate some security metrics, but it is unclear *how* different metrics contribute to the overall risk value. Moreover, risk analysis is blamed for providing results with low precision and consuming huge amount of time [10]. In some situations, usage only of security metrics contributing to the overall risk value may facilitate the analysis and make a preliminary assessment.

1.1 Contribution

In our previous work [13] we provided a formal description of various security metrics which relate only to a system (out of context) and investigated the relations between them. We have found that though some metrics are influenced by other metrics, in a wide sense, the existing metrics measure distinct aspects of security. On the other hand, the metrics must contribute to the overall security level. In contrast, in this work we have the main goal to establish the relation between security metrics and the most general and high-level way of security assessment – risk analysis. The formal model we propose explicitly connects various security metrics and indicates how they contribute to the overall assessment. Note, that we do not provide a new security assessment method, but analyse the existing ones.

The paper is organised as follows. In Section 2 we recall our definition of perfectly secure system, which we defined in [13], and describe our attack model. Section 3 is devoted to our formal definition of risk. Section 4 establishes the connection between the probability of successful exploitation of an attack and two types of cost. We analyse contributions of existing metrics to risk in Section 5. Related work (Section 6) and Conclusion (Section 7) conclude the paper.

2 Background

Definition 1. *Let $\mathcal{S}$ be a process modelling behaviour of a system and $\mathcal{X}$ a process modelling behaviour of an attacker. A system and an attacker perform some actions $a_l \in A$ and move from one state to another one. We denote a trace of actions accomplished by a system or an attacker as γ ($\gamma \in \Gamma$). $\gamma' \bullet \gamma'_{\mathcal{X}}$ denotes that one trace of actions is merged with another one in any way preserving the order of events. We say that the system is (perfectly) secure if and only if*

$$\forall \mathcal{X},\ \forall \gamma,\ \mathcal{S} \xrightarrow{\gamma'} \mathcal{S}'\ \wedge\ \mathcal{X} \xrightarrow{\gamma'_{\mathcal{X}}} \mathcal{X}',\ \gamma = \gamma' \bullet \gamma'_{\mathcal{X}}$$
$$\mathcal{S} \| \mathcal{X} \xrightarrow{\gamma} \mathcal{S}' \| \mathcal{X}' \Rightarrow P_{sec}(\mathcal{S}' \| \mathcal{X}') = \emptyset \quad (1)$$

Function $P_{sec}(\mathcal{S}'\|\mathcal{X}')$ returns the set of possible threats (attacker's goals) which may occur in the reached state $\mathcal{S}'\|\mathcal{X}'$ when the system and the attacker work in parallel. In other words, the attacker has achieved a state where some malicious actions are possible and valuable assets can be compromised (e.g., the attacker has access to a database). A set of possible attackers is $\mathbf{X}$. We define an attacker $\mathcal{X}$ simply as a set of possible traces the attacker can launch against the system. We write $\gamma \in \mathcal{X}$ to show that a specific attacker knows the trace (attack). We also use $a \in \gamma$ notation to denote that action a is contained in trace γ. A trace of events is denoted in the following way preserving the order of actions: $\gamma = a_1 \circ a_2 \circ \cdots \circ a_n$. To avoid ambiguity, we always use index l for actions, i for attacks, j for attackers.

In this work we extend our previous model and consider security of a system in a specific context. In our current model context includes protected assets and possible attackers. In particular, we need the amount of possible losses, caused by affecting valuable assets, and preferences of attackers.

For our new model we need a more detailed formal model of attacker.

Definition 2. *An attacker is a process which is characterised by the following tuple:* $\mathcal{X} =< \Gamma, goal, skill, res, money >$*, where* Γ *is a set of attacks the attacker can launch against the system; goal is the goal of the attacker*[3]*; skill - the level of skills the attacker possesses;* res *- the amount of resources the attacker is willing to spend to achieve its goal; money is the amount of money the attacker is ready to spend in order to* make an attempt *to compromise the system.*

Here we would like to consider money ($money$) and resources (res) required for an attack apart. In our model, money are needed for buying the tools without which the attack is impossible (e.g., in order to crack a safe a special drill is required). When the attacker starts its attack he spends some resources in order to achieve its goal. The more resources are spent the more chances for success the attacker has (e.g., the more time a bugler spends for studying and attempting to open a lock the more probably he will be able to open the safe). Sometimes money and resources can be considered as one parameter, but for understanding the different nature of these expenditures we consider them as two distinct sets. In the sequel, any attribute of a specific attacker is used with a corresponding index. For example, a set of possible attacks and amount of available resources for an attacker $\mathcal{X}_j$ are represented as Γ_j and res_j correspondingly.

Considering every attacker separately is an impractical approach. Usually similar attackers considered as one collective entity, or an attacker profile. We assume that all members of the same group of attackers have the same goal. For example, cyber terrorists are aimed at shutting down a system for a long time, cyber thieves (hackers) - at receiving economical benefits, insiders - at committing a fraud. Thus, we group the attackers according to their goals assuming that the attackers which have the same goal have also the same skills and resources (i.e., we assume small dispersion). Sometimes, there are attacker profiles which

[3] In our model every attacker has only one goal

have the same goal but should be grouped differently (e.g., terrorists which usually have high skills and large amount of resources, and vandals, who simply behave as hooligans and have very limited amount of resources). Such groups can be separated, and this separation will not affect our further discussions.

3 Formal definition of risk

Let the total number of attackers be $|\mathbf{X}| = N^{\mathbf{X}}$ and number of attacks available for attackers $\mathcal{X}_j \in \mathbf{X}$ is $|\Gamma_j| = N_j^{\Gamma}$. Now, let a number of attacker profiles be $N^{\mathbf{X},pr}$ and each profile j has $|\mathcal{X}_j| = N_j^{\mathbf{X}}$ attackers ($N^{\mathbf{X}} = \sum_{j=1}^{N^{\mathbf{X},pr}} N_j^{\mathbf{X}}$).

Definition 3.

$$\forall \mathcal{X}_j \in \mathbf{X}, \forall \gamma_i \in \Gamma_j,\ \exists \gamma'\ \mathcal{S} \xrightarrow{\gamma'} \mathcal{S}'\ \wedge\ \mathcal{X} \xrightarrow{\gamma_i} \mathcal{X}',$$

$$\mathcal{S}\|\mathcal{X} \xrightarrow{\gamma' \bullet \gamma_i} \mathcal{S}'\|\mathcal{X}' \Rightarrow P_{sec}(\mathcal{S}'\|\mathcal{X}') \ni goal_j$$

$$Risk(\mathcal{S}) = \sum_{j=1}^{N^{\mathbf{X},pr}} N_j^{\mathbf{X}} \times \sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j) \times d(\gamma_i, \mathcal{X}_j) \tag{2}$$

where $p^v(\gamma_i, \mathcal{X}_j)$ is the probability of successful execution of attack γ_i by $\mathcal{X}_j$;
$p^t(\gamma_i, \mathcal{X}_j)$ is the probability of selection of attack γ_i by $\mathcal{X}_j$;
$d(\gamma_i, \mathcal{X}_j)$ is the damage which $\mathcal{X}_j$ causes by successfull execution of γ_i.

Note, that an attacker which is going to attack the system has to select one of the available attacks leading to achievement of its goal. Therefore, we have complete probability space here: $\forall \mathcal{X}_j,\ \sum_{i=1}^{N_j^{\Gamma}} p^t(\gamma_i, \mathcal{X}_j) = 1$. On the contrary, probability of successful execution of an attack does not depend on other attacks, but only on the attacker and the attack. Therefore, the complete probability space for the probability of successful execution of attack γ_i by $\mathcal{X}_j$ is $p^v(\gamma_i, \mathcal{X}_j)$ and $\neg p^v(\gamma_i, \mathcal{X}_j)$.

If we know that a randomly taken attacker belongs to group $\mathcal{X}_j$ with probability $p_j^{\mathbf{X}}$ we can find the number of attackers in this group if the overall amount of attackers is known.

$$N_j^{\mathbf{X}} = N^{\mathbf{X}} * p_j^{\mathbf{X}} \tag{3}$$

Naturally, $\sum_{j=1}^{N^{\mathbf{X},pr}} p_j^{\mathbf{X}} = 1$

Proposition 1. *Definition 3 is a fine-grained form of the classical formula for computation of risk (annualised losses) [6, 10]:*

$$Risk(\mathcal{S}) = \sum_{j=1}^{N^{\mathbf{X},pr}} ARO_j * SLE_j \tag{4}$$

Where ARO_j is annual rate of occurrences of threat j ($goal_j$) and SLE_j is single loss expectancy of threat j.

Proof First, we consider ARO_j. ARO_j gives us the average number of successful attacks which realise threat j. Let p_j^{real} be the probability that the next attack is successful in realisation of threat j. Then, the *number* of successful attacks can be found if a number of all attackers (attempts to compromise the system) and probability p_j^{real} are known $ARO_j = N^{\mathbf{X}} \times p_j^{real}$. To execute an attack an attacker has to *select* the threat and then *successfully realise* it. Therefore, expanding p_j^{real} ARO_j can be seen as $ARO_j = N^{\mathbf{X}} \times Vuln_j \times Threat_j$, where $Vuln_j$ is the average probability that threat j is *successfully realised*; $Threat_j$ is the probability that threat j is *selected*.

The selection of threat j is equivalent to the probability that the selected attacker is from profile j (recall that a "threat" and an "attacker goal" in our work are synonymous), therefore, $Threat_j = p_j^{\mathbf{X}}$. Using the probability theory we can compute the average probability that a concrete threat will be successful if we know all attacks which lead to realisation of this threat (goal). This set of attacks is the same set that a specific group of attackers knows.

$$Vuln_j = \sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j) \tag{5}$$

SLE_j is the expected damage in case threat j occurs. Note, that SLE_j is the average damage with *the condition that the attack is successful*. Indeed, in practice, the average damage is computed using the data collected from previous occurrences of threats. Therefore, we need to use *conditional* probabilities for computation of the average damage. Thus, the probability that attack γ_i has successfully occurred with the condition that at least one attack realising threat j has occurred is $p(\gamma_i/\Gamma_j) = \frac{p(\gamma_i)}{p(\Gamma_j)}$, where $p(\gamma_i)$ is the probability that attack γ_i is successfully executed, and $p(\Gamma_j)$ is the probability that one attack out of Γ_j has been successful. Thus, the formula for computation of SLE_j is the following:

$$SLE_j = \sum_{i=1}^{N_j^{\Gamma}} \frac{p(\gamma_i)}{p(\Gamma_j)} \times d(\gamma_i, \mathbf{X}_j) = \sum_{i=1}^{N_j^{\Gamma}} \frac{p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j) \times d(\gamma_i, \mathcal{X}_j)}{\sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j)} \tag{6}$$

Now, if we multiply and divide at once the part of formula 2 after the first sum by $\sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i, \mathcal{X}_j) p^t(\gamma_i, \mathcal{X}_j)$ and substitute $N_j^{\mathbf{X}}$ as shown in Equation 3:

$$\begin{aligned} Risk(\mathcal{S}) = N^{\mathbf{X}} \times \sum_{j=1}^{N^{\mathbf{X},pr}} [p_j^{\mathbf{X}} \times \\ (\sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j)) \times \frac{\sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j) \times d(\gamma_i, \mathcal{X}_j)}{\sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j)}] \end{aligned} \tag{7}$$

Finally, using Equations 5 and 6 and recalling that $Threat_j = p_j^{\mathbf{X}}$ we get:

$$Risk(\mathcal{S}) = N^{\mathbf{X}} \times \sum_{j=1}^{N^{\mathbf{X},pr}} Threat_j \times Vuln_j \times SLE_j = \sum_{j=1}^{N^{\mathbf{X},pr}} ARO_j \times SLE_j \quad (8)$$

□

4 Probability vs. Cost

Cost of attack is a metric which is often used for analysis of security. Cost is considered as a one-time payment which an attacker has to make in order to exploit a vulnerability. An example could be the average amount of money required for bribing an employee in order to get access to the network or to buy information about an unknown vulnerability on a black market [21]. Such model is not entirely correct. First, one-time payment is usually an indispensable condition, but not a sufficient one. Possessing the information about an existing vulnerability and required tools do not always imply its successful exploitation. Second, in many cases different amount of investments may result in different probabilities of success. For example, the higher the bribe the higher the probability it is accepted. Third, in contrast to the real world criminals (e.g., buglers or thieves), hackers do not often need special equipment, but a computer, tools (likely, simply downloaded) and access to the Internet (or to the internal network). In other words, exploitation of most of vulnerabilities often does not require one-time investments.

Therefore, in this paper we propose to consider two types of cost: a fixed cost (C^f) and a changing cost (C^c). The first cost is the common one-time investment. Such investment is required to allow the attacker to make an attempt to exploit a vulnerability. The changing cost is the investment which influences the probability of successful exploitation of a vulnerability. Such investment is often only the time the attacker devotes to exploitation of a vulnerability. We can express this time in currency by simple multiplication of the time spent by the cost of an hour of the attacker (a way of transformation does not affect the further discussion). The idea behind this cost is the following one: anyone can exploit a vulnerability spending some time trying to do this (see, for example, the work of E. Jonsson and T. Olovsson [11] where even unskilled attackers were able to compromise the system after considerable time).

In order to model such dependency we can use either lognormal [18] or Weibull distributions. Both these distributions are used for modelling faults. In our case we can see the problem as how long the system withstands an attack. We also can apply multiplicative degradation argument here. In every small amount of time an attacker gets a tiny amount of knowledge about how to exploit a vulnerability. In this case system is "degrading" until it is broken. Such degradation is modelled by lognormal distribution [1].

We define the probability of successful execution of action a_l as a function of cost C_l^c and specific for the attacker profile (attacker skill level): $p^c(a_l, \mathcal{X}_j) =$

$F_{j,l}(C_l^c)$, where $F_{j,l}$ is some distribution function (the exact formula, although desirable, is not important for the further discussion). We assume that this function depends on such attributes as, e.g., hardness of the exploitation of a_l and skill level of the attacker ($skill_j$). The function returns the probability that the action will be successful when at most C^c amount of resources is spent.

Definition 4. *The probability of successful attack is the maximal probability to accomplish successfully all required actions, if the overall sum of resources spent for the overall attack is equal to the amount of resources the attacker has.*

$$p^v(\gamma_i, \mathcal{X}_j) = max\{ \prod_{\forall a_l \in \gamma_i} F_{j,l}(C_l^c) | \sum_{\forall a_l \in \gamma_i} C_l^c = res_j\} \tag{9}$$

The fixed cost is used for defining the set of attacks available for the attacker:

$$\begin{aligned} &\Gamma_j = \{\gamma_i \mid \exists \gamma',\ \mathcal{S} \xrightarrow{\gamma'} \mathcal{S}' \ \wedge\ \mathcal{X} \xrightarrow{\gamma_i} \mathcal{X}', \\ &\mathcal{S}\|\mathcal{X} \xrightarrow{\gamma' \bullet \gamma_i} \mathcal{S}'\|\mathcal{X}' \Rightarrow P_{sec}(\mathcal{S}'\|\mathcal{X}') \ni goal_j \ \wedge \sum_{\forall a_l \in \gamma_i} C_l^f \leq money_j\} \end{aligned} \tag{10}$$

Minimal cost of attack (see Definition 11) has sense only for the fixed cost (C^f), but as we noted, possessing this amount of money does not always guarantee successful exploitation. The changing cost (C^c) simply cannot be minimal because even with a little effort an attacker has a chance (but a very small chance) to achieve its goal. Example could be the password cracker who finds a strong password after a couple of attempts by sheer luck.

5 Relation between metrics and risk

First, we define four levels of relations which can be established between two metrics. For brevity, lets call the metric which we observe and use for defining the dependency as a *dependee metric*, when the metric which behaviour we would like to determine as a *depender metric*.

Definition 5. *Let $\mathcal{S}$ and $\hat{\mathcal{S}}$ be the system before and after some changes. Correspondingly, $M(\mathcal{S})$ and $M(\hat{\mathcal{S}})$ are values of a dependee metric for the two versions. We can denote a depender metric as a function which depends on the dependee metric $f(M(\mathcal{S}))$ or $f(M(\mathcal{S}), M_1(\mathcal{S}), ..., M_n(\mathcal{S}))$ depending on how many dependee metrics are required for the computation. Let also $\triangle M(\mathcal{S})$ be the simplest change of the dependee metric $M(\mathcal{S})$ such that no other changes may occur at the same time.*

Level 1 . *Weakest monotonicity. There is a weakest monotonicity relation between a depender and dependee metrics if the smallest increases of dependee metric cause the corresponding changes of the depender metric, while all*

other parameters required for computation of the depender metric are left the same. Formally,

$$\begin{aligned} &\textit{If } M(\hat{\mathcal{S}}) = M(\mathcal{S}) + \triangle M(\mathcal{S}) \ , \ M(\hat{\mathcal{S}}) > M(\mathcal{S}) \Rightarrow \\ &f(M(\hat{\mathcal{S}}), M_1(\hat{\mathcal{S}}), ..., M_n(\hat{\mathcal{S}})) > f(M(\mathcal{S}), M_1(\mathcal{S}), ..., M_n(\mathcal{S})) \\ &\forall k, \ M_k(\hat{\mathcal{S}}) = M_k(\mathcal{S}) \end{aligned} \tag{11}$$

Level 2 . *Weak monotonicity. There is a weak monotonicity relation between two metrics if any resulting changes of dependee metric allows to judge about changes in the depender metric. All other parameters required for computation of the depender metric are left the same. Formally,*

$$M(\hat{\mathcal{S}}) > M(\mathcal{S}) \Rightarrow f(M(\hat{\mathcal{S}}), M_1(\hat{\mathcal{S}}), ..., M_n(\hat{\mathcal{S}})) > f(M(\mathcal{S}), M_1(\mathcal{S}), ..., M_n(\mathcal{S})) \tag{12}$$

$$\forall k, \ M_k(\hat{\mathcal{S}}) = M_k(\mathcal{S})$$

Level 3 . *One-way monotonicity. Changes of dependee metric imply corresponding changes in the depender metric, even if we consider different systems (other parameters, if any, may change as well). Formally,*

$$M(\hat{\mathcal{S}}) > M(\mathcal{S}) \Rightarrow f(M(\hat{\mathcal{S}})) > f(M(\mathcal{S})) \tag{13}$$

Level 4 . *Equivalence. Changes of dependee metric imply corresponding changes in the depender metric, and visa versa:*

$$M(\hat{\mathcal{S}}) > M(\mathcal{S}) \Leftrightarrow f(M(\hat{\mathcal{S}})) > f(M(\mathcal{S})) \tag{14}$$

The four levels are defined for monotonically increasing functions only for simplicity. Monotonically decreasing functions can be also used by the definitions (simply change $M(\hat{\mathcal{S}}) > M(\mathcal{S})$ to $M(\hat{\mathcal{S}}) < M(\mathcal{S})$).

Naturally, the first two levels are more relevant for considering the relations when a depender metric is a function of several dependee metrics, while the last two levels are applicable when only one dependee metric is required. Knowing what kind of relations exists between two metrics an analyst is able to predict changes of a more complex metric observing changes in another one (more easy to collect). Every monotonic relation can be either *sensitive* or *insensitive*.

Definition 6. *Sensitive relation notices every change in the dependee metric behaviour. A monotonic relation is insensitive otherwise.*

For example, weak monotonicity is *sensitive* if

$$M(\hat{\mathcal{S}}) > M(\mathcal{S}) \Rightarrow f(M(\hat{\mathcal{S}}), M_1(\hat{\mathcal{S}}), ...) > f(M(\mathcal{S}), M_1(\mathcal{S}), ...) \tag{15}$$

and insensitive if

$$M(\hat{\mathcal{S}}) > M(\mathcal{S}) \Rightarrow f(M(\hat{\mathcal{S}}), M_1(\hat{\mathcal{S}}), ...) \geq f(M(\mathcal{S}), M_1(\mathcal{S}), ...) \tag{16}$$

Now, our goal is to find how changes in security metrics affect risk level.

Number of attacks.

Definition 7. *We define* number of attacks *metric as the number of possible sequences of actions which contain the minimal number of actions required for satisfaction of attacker's goal.*

$$N_{att}(\mathcal{S}) = |\{\gamma'_i \mid \exists \mathcal{X}_j \in \mathbf{X},\ \gamma'_i \in \Gamma'_j\ \exists \gamma',\ \mathcal{S} \xrightarrow{\gamma'} \mathcal{S}'\ \wedge\ \mathcal{X}_j \xrightarrow{\gamma'_i} \mathcal{X}'_j \wedge$$
$$\mathcal{S} \| \mathcal{X}_j \xrightarrow{\gamma' \bullet \gamma'_i} \mathcal{S}' \| \mathcal{X}'_j \Rightarrow P_{sec}(\mathcal{S}' \| \mathcal{X}'_j) \ni goal_j \wedge \tag{17}$$
$$\nexists \hat{\gamma}'_i, \hat{\gamma},\ \gamma'_i = \hat{\gamma}'_i \bullet \hat{\gamma}\ \wedge\ \mathcal{S} \| \mathcal{X}_j \xrightarrow{\gamma' \bullet \hat{\gamma}'_i} \mathcal{S}' \| \mathcal{X}'_j \Rightarrow P_{sec}(\mathcal{S}' \| \mathcal{X}'_j) \ni goal_j\}|$$

Proposition 2. *There is only the insensitive weakest monotonicity between risk and number of attacks metric (Level 1).*

Proof Consider two cases. The first case is when all Γ_j contain only the attacks the attackers can afford (see Equation 10). Thus, the attack can be executed (otherwise $\gamma_i \notin \Gamma_j$) and $p^v(\gamma_i, \mathcal{X}_j) \neq 0$; can be selected, even with very small probability, (otherwise $\gamma_i \notin \Gamma_j$) and $p^t(\gamma_i, \mathcal{X}_j) \neq 0$; and has some impact on the system (otherwise we do not consider it as an attack $\gamma_i \notin \Gamma_j$ and $d(\gamma_i, \mathcal{X}_j) \neq 0$. Thus, if the number increases ($\triangle N_{att}(\mathcal{S}) > 0$) more summands ($p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j) \times d(\gamma_i, \mathcal{X}_j)$) will contribute to the overall risk and the risk level increases. If the number decreases then less summands contribute to the risk and the risk level decreases. Note, the change of risk because of several changes in number of attacks is unpredictable (because the value of the summands is unknown).

In the second case we assume that some attacks are too expensive for attackers. Thus, there are attacks with 0 impact and the situation when $\triangle f(N_{att}(\mathcal{S})) = 0$ is possible and new summands are not added/deleted when number of attacks metric changes. Thus, in some situation the relation is insensitive. □

Maximal probability of success. In this paper we provided a new definition for probability of successful exploitation shown in Equation 18 (using $p^v(\gamma'_i, \mathcal{X}_j)$ from Equation 9)

Definition 8. *This metrics is simply the maximal probability of successful exploitation of one of possible attacks.*

$$P^{max}(\mathcal{S}) = max\{p^v(\gamma_i, \mathcal{X}_j) \mid \forall \mathcal{X}_j, \gamma_i \in \Gamma_j\} \tag{18}$$

Proposition 3. *Risk is an insensitive weak monotonic function of maximal probability of success (Level 2).*

Proof Maximal probability of success $P^{max}(\mathcal{S})$ is just one of the probabilities of execution used for computation of risk. Therefore, if $P^{max} = p^v(\gamma_q, \mathcal{X}_z)$ for

an attack γ_q ($\gamma_q \in \Gamma_z$) conducted by attacker $\mathcal{X}_z$ we can see the Equation 2 as

$$Risk(\mathcal{S}) = \sum_{j=1}^{N^{\mathbf{X},pr}} N_j^{\mathbf{X}} \times \sum_{\forall i \neq q} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j) \times d(\gamma_i, \mathcal{X}_j) + \sum_{\forall j \neq z \ . \ \gamma_q \in \Gamma_j} N_j^{\mathbf{X}} \times p^v(\gamma_q, \mathcal{X}_j) \times p^t(\gamma_q, \mathcal{X}_j) \times d(\gamma_q, \mathcal{X}_j) + N_z^{\mathbf{X}} \times P^{max} \times p^t(\gamma_q, \mathcal{X}_z) \times d(\gamma_q, \mathcal{X}_z) \quad (19)$$

Thus, clearly, if $P^{max}(\mathcal{S})$ increases/decreases the overall risk decreases/increases only if all other parameters are left the same (Level 2). Note, that if the attack with maximal cost is too costly for the corresponding attackers than no changes will be noticed. □

Shortest attack.

Definition 9. *The shortest attack metrics indicates the length of an attack which contains less actions than others.*

$$L^{min}(\mathcal{S}) = min\{L(\gamma_i) \mid \forall \mathcal{X}_j, \gamma_i \in \Gamma_j\} \quad (20)$$
$$where\ L(\gamma) = n\ iff\ \gamma = a_1 \circ a_2 \circ \cdots \circ a_n$$

Proposition 4. *There is only the insensitive weakest monotonicity between risk and the shortest attack metric (Level 1).*

Proof The shortest attack $L^{min}(\mathcal{S})$ affects only the probabilities which correspond to the same attack γ_q $\{p^v(\gamma_q, \mathcal{X}_j), \forall j\}$. If the shortest attack becomes longer/shorter the corresponding probabilities will decrease/increase according to Definition 8. We isolate all the affected summands in Equation 2.

$$Risk(\mathcal{S}) = \sum_{j=1}^{N^{\mathbf{X},pr}} N_j^{\mathbf{X}} \times \sum_{\forall i \neq q} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j) \times d(\gamma_i, \mathcal{X}_j) \sum_{\forall j \ . \ \gamma_q \in \Gamma_j} N_j^{\mathbf{X}} \times p^v(\gamma_q, \mathcal{X}_j) \times p^t(\gamma_q, \mathcal{X}_j) \times d(\gamma_q, \mathcal{X}_j) \quad (21)$$

Thus, only the second sum descreases/increases when L^{min} increases/decreases. Note, that the shortest attack affects probabilities of success only if it has been either increased or decreased (not both at the same time) because of different magnitudes of changes in the probabilities. In other words, we have relation of Level 1. And, again, the change is noticeable only if the attack is not too expensive. □

Percentage of compliance. Some authors propose to measure security according to its compliance with a standard (e.g., ISO 17799[4] [8]). Percentage of compliance is often used as an indicator [4].

[4] Currently, the standard has been extended and is called ISO 27000 family.

Definition 10. *Check list is a set of actions recommended for a system* $\Gamma^{cl} \subseteq \Gamma$. *Let a set of satisfied items in the list be* $\Gamma^S = \{\gamma | \gamma \in \mathcal{S} \ \wedge \ \gamma \in \Gamma^{cl}\}$. *The check list metric is the following ratio*

$$CLM(S) = |\Gamma^S|/|\Gamma^{cl}| \tag{22}$$

Proposition 5. *There is only the insensitive weakest monotonicity between risk and the percentage of compliance metric (Level 1).*

Proof Since we consider a static system we will not take into account the requirements related to a process of security maintenance. Lets also assume that adding a new countermeasure does not have any negative effect on security of the system. We already have shown in [13] that this metric is not sensitive because some suggested countermeasures could be ineffective in a concrete system.

Every security mechanism may work in three ways:

1. reduce the probability of successful exploitation of some vulnerabilities (e.g., password generation policies) – $p^v(\gamma_i, \mathcal{X}_j)$;
2. reduce the amount of attackers willing to perform a specific attack (e.g., monitoring mechanisms). Such security mechanisms have double effect:
   (a) reduce the probability of attack selection $p^t(\gamma_i, \mathcal{X}_j)$ and
   (b) reduce the total amount of attackers $N_j^{\mathbf{X}}$ which know the attack;
3. reduce the possible impact (e.g., back up mechanisms) $d(\gamma_i, \mathcal{X}_j)$.

Reduction of amount of attackers caused by installation of a new security mechanism causes redistribution of p^t-s, since $\sum_{\forall i} p^t(\gamma_i, \mathcal{X}_j) = 1$. In this article, we follow the strategy common for risk assessment methodologies: some attackers are no longer a threat for the system. We do not consider a more complex scenario when an attacker changes its mind and tries another attack [22]. Such analysis requires deeper understanding of how probabilities of selection are determined using behaviour of attacker. We are going to consider this issue in the future work.

Current redistribution of probabilities is connected only with reduction of one probability of selection caused by $\triangle CLM(S)$. In order to simplify mathematics and avoid re-computation of the probabilities, for our proof is enough just to imagine that we have a bogus attack with risk 0, but its probability of selection is a non-zero value $p_0^t > 0$. Thus if some $p^t(\gamma_i, \mathcal{X}_j)$ has been reduced by $\triangle p^t$ we simply add this value to the zero attack: $p_0^t + \triangle p^t$. In such a way we reduce only the summands which correspond to attack γ_i and, as a result, the risk reduces.

For reduction of other parameters (probability of successful exploitation and impact) similar to arguments for the shortest attack metric we can separate the summands which are affected by new countermeasures (or by deletion of countermeasures). The separated summands decrease if new countermeasures are installed and, thus, risk decreases. □

Minimal cost of attacks. As we have shown in Section 4 minimal cost makes sense only for the fixed cost.

Definition 11. *Minimal fixed cost of attack can be see as:*

$$C^{f,min}(\mathcal{S}) = min\{\sum_{\forall a_l \in \gamma_i} C_l^f \mid \forall \mathcal{X}_j, \gamma_i \in \Gamma_j\} \tag{23}$$

Proposition 6. *Risk is an insensitive weak monotonic function of minimal fixed cost metric (Level 2).*

Proof This cost affects only the process of selection of available attack paths (see Equation 10). In other words, the attack which had a minimal cost value may become too expensive for an attacker if the minimal cost value increases. In this case, the formula for risk loses one non-negative summand and risk decreases. Note, that if the increase in the cost is small and the attacker still can use the attack risk level is left the same. □

Average probability of penetration.

Definition 12. *In order to find the average probability of penetration for the whole systems we should first find the average probability for an attacker profile and then find the average probability of penetration among the attacker profiles.*

$$P^{avg}(\mathcal{S}) = \sum_{j=1}^{N^{\mathbf{X},pr}} p_j^{\mathbf{X}} \times \sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i, \mathcal{X}_j) \times p^t(\gamma_i, \mathcal{X}_j) \tag{24}$$

Proposition 7. *There is only the sensitive weakest monotonicity between risk and the average probability of penetration metric (Level 1).*

Proof Although this metric uses the same components as risk does, there is no direct relation between risk and this metrics. Effects of changes of p^t and p^v have been discussed in the proof for percentage of compliance metric. Increase of number of attackers of one kind ($p_j^{\mathbf{X}}$) increases the average probability of penetration and risk (see Equations 2 and 3). In general, without knowledge of exact magnitudes of changes in several probabilities we cannot correctly predict behaviour of risk level, since risk is weighted with impact. Thus, we have a relation of Level 1. Since risk reacts on the change of every parameter required for P^{avg} the relation is sensitive. □

Attack surface metric. Attack surface metric (ASM) [17] is defined as follows.

Definition 13. *Let us have 3 assets which can be affected by an attack:* method (m), data items (d), channel (c). *Let us know the damage-potential level of every asset* $dam^p(\gamma)$ *and the level of privileges required for execution of attack* γ_i $priv(\gamma_i)$ *(maximal difference in level of privileges among required actions*

of the same attack). Then, for every system we can assign the following tuple $ASM(S) = \langle Risk^m, Risk^c, Risk^d \rangle$ *where*

$$Risk^m = \sum_{\forall \gamma_i \in \Gamma^m} \frac{dam^p(\gamma_i)}{priv(\gamma_i)};\ Risk^c = \sum_{\forall \gamma_i \in \Gamma^c} \frac{dam^p(\gamma_i)}{priv(\gamma_i)};$$
$$Risk^d = \sum_{\forall \gamma_i \in \Gamma^d} \frac{dam^p(\gamma_i)}{priv(\gamma_i)}). \tag{25}$$

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

Proposition 8. *Attack surface metric is equivalent to risk with a number of assumptions (Level 4).*

Proof Since there are three values required for computation of ASM we also can compute risk for three possible damages separately. Assume that there are no attacks on the system others than the ones targeting the three assets ($N^{\mathbf{X},pr} = 3$). The authors assume that the metric does not depend on the attacker. Thus, we do the same assumption for our risk formula. The authors also assume that the damage-potential value is proportional to the real value of loss, and the required level of privileges is reversely proportional to the probability to perform the attack: $dam^p(\gamma_i) = z1 * d(\gamma_i)$ and $priv(\gamma_i) = z2/p^v(\gamma_i)$. Here we have to make another assumption: all assets of the same class have the same cost and an attack required the same level of privileges have the same probability to be successful. Finally, we get almost the same formula we have for risk, but one compound: threat level. In other words, we also need an assumption that all attacks are equally frequent ($\forall \gamma_i\ p^t(\gamma_i) = p^t$). Now we can rewrite equation 2 using the assumptions we already made:

$$Risk(\mathcal{S}) = \sum_{j=1}^{N^{\mathbf{X},pr}} N_j^{\mathbf{X}} \times \sum_{i=1}^{N_j^{\Gamma}} p^v(\gamma_i) \times p^t(\gamma_i) \times d(\gamma_i) =$$
$$\sum_{j=1}^{N^{\mathbf{X},pr}} N_j^{\mathbf{X}} \times \sum_{i=1}^{N_j^{\Gamma}} p^t \times z2/priv(\gamma_i) \times dam^p(\gamma_i)/z1 = p^t \frac{z2}{z1} \times$$
$$(N_m^{\mathbf{X}} \sum_{\forall \gamma_i \in \Gamma^m} \frac{dam^p(\gamma_i)}{priv(\gamma_i)} + N_c^{\mathbf{X}} \sum_{\forall \gamma_i \in \Gamma^c} \frac{dam^p(\gamma_i)}{priv(\gamma_i)} + N_d^{\mathbf{X}} \sum_{\forall \gamma_i \in \Gamma^d} \frac{dam^p(\gamma_i)}{priv(\gamma_i)}) \tag{26}$$

Here we have the overall risk, while ASM does not combine the three values together. We can do the same considering the three summands separately. □

Summary In order to summarise the results we collect the findings in Table 1. We can see that most metrics have only the lowest level of relation with risk (weakest monotonicity). Thus, usage of only these metrics in order to predict the behaviour of risk level is impractical, although, changes of these metrics do

Metric	Relation level	Sensitivity
Number of attacks N_{att}	Level 1	No
Maximal probability P^{max}	Level 2	No
Shortest attack L^{min}	Level 1	No
Minimal fixed cost $C^{f,min}$	Level 2	No
Avg. probability of penetration P^{avg}	Level 1	Yes
Attack surface ASM	Level 4	Yes
Percentage of compliance CLM	Level 1	No

Table 1. Relations between metrics and risk

contribute to changes of risk. Maximal probability and minimal fixed cost could be used for prediction of risk behaviour, but only if the corresponding attacks are considered. Such situation happens if attackers always select the most probable or less costly attack. Finally, we see that attack surface metric is equivalent to computation of risk, but relies on very strong assumptions. Moreover, most relations are insensitive and, thus, changes of the metrics do not always indicate change of risk.

6 Related work

Most security metrics are defined informally. Such definition leads to many uncertainties in the actual meaning of the metrics. Informal definitions also do not allow to analyse metrics, find overlapping and relations between them. Unsurprisingly, NIST stated that one of the future directions in security metrics should be definition of formal models for security metrics [9].

An example of formally defined metric could be the attack surface metric [15, 17]. The authors formally defined the notion of channels (attack path) introducing the notion of exit points and described how the metric is computed. In our work, we adapted the model of the authors to our model and formally proved that this metric is equivalent to risk, if the specified assumptions are taken into account. Nevertheless, the focus of our paper is formal analysis of large number of existing metrics, while the authors of attack surface metric focus on definition of this metric.

The authors of papers on attack graphs are also often use formal models. Moreover, a number of security metrics are defined for evaluation of a system based on attack graphs are: probability of successful attack [26], minimal cost of attack [20], minimal cost of reduction [27], shortest path [19]. The formal model is usually applied to the definition of the graph itself and only rarely used for the definition of metrics (e.g., [20]). In contrast, our work has the primary focus on formal definition and analysis of metrics.

Another example of formally defined metric is “mean time to failure” metric by Madan et al. [14]. This metric assumes that only one-step attacks are possible, when we consider multi-step attacks.

In our previous work [13] we formally modelled and defined several security metrics which measure security system out of the context. The metrics were analysed in order to check if some of them provide the same evaluation. We have found that in general metrics are mostly independent, but in specific cases some metrics can be used interchangeably. In this work, we formalised risk and have shown how these (and some other) metrics contribute to risk.

7 Conclusion

In this paper we formalised risk analysis. We have shown how existing security metrics relate to this the most general security evaluation. We can see that all metrics play only a small role when the overall risk is computed. Thus, we make a conclusion that none of single metrics is enough to predict behaviour of the risk value. The only metric which is as general as risk is the attack surface metric, but it relies on many strong assumptions. In this work we considered probability of successful execution of an attack as a function of cost. We have not identified which function must be used, but have shown that other approaches fail to model the relation between these two metrics correctly.

Currently, we consider a very generic attacker model. Our future work is to consider behaviour of attackers and determine models for computation of probabilities of attack selection. Introducing the behaviour of attackers (e.g., adapting Dolev-Yao model for assessment of systems) will enhance our attacker model and will allow us to analyse different strategies of attackers. The probability of attack selection is often left out of the scopes of existing approaches and we are going to make some progress to fill this gap.

References

1. S. J. Bae, et. al. Degradation models and implied lifetime distributions. *Reliability Engineering & System Safety*, 92(5):601 – 608, 2007.
2. S. A. Butler. Security attribute evaluation method: a cost-benefit approach. In *Proceedings of the 24th International Conference on Software Engineering (ICSE'02)*, pages 232–240. ACM Press, 2002.
3. V. Casola et. al. A SLA evaluation methodology in Service Oriented Architectures. In *Proceedings of the 1st Workshop on Quality of Protection.*, Milan, Italy, 2005. Springer-Verlag.
4. M. M. Eloff and S. H. von Solms. Information security management: An approach to combine process certification and product evaluation. *Computers & Security*, 19(8):698–609, 2000.
5. L. Gordon and M. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457, 2003.
6. L. A. Gordon and M. P. Loeb. *Managing Cybersecurity Resources: a Cost-Benefit Analysis.* McGraw Hill, 2006.
7. D. S. Herrmann. *Complete Guide to Security and Privacy Metrics. Measuring Regulatory Compliance, Operational Resilience, and ROI.* Auerbach Publications, 2007.

8. ISO/IEC. *ISO/IEC 27002:2005 Information technology – Security techniques – Code of Practice for Information Security Management*, 2005.
9. W. Jansen. Directions in security metric research. Technical Report NISTIR 7564, National institute of Standards and Technology, 2009.
10. A. Jaquith. *Security metrics: replacing fear, uncertainty, and doubt.* Addison-Wesley, 2007.
11. E. Jonsson and T. Olovsson. A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering*, 23(4):235–245, 1997.
12. G. Karjoth, et. al. Service-oriented assurance comprehensive security by explicit assurances. In *Proceedings of the 1st Workshop on Quality of Protection.*, Milan, Italy, September 2005. Springer-Verlag.
13. L. Krautsevich, et. al. Formal approach to security metrics. what does "more secure" mean for you? In *Proceedings of the 1st International Workshop on Measurability of Security in Software Architectures*. ACM Press, 2010.
14. 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.
15. P. Manadhata and J. Wing. Measuring a system's attack surface. Technical Report CMU-TR-04-102, Carnegie Mellon University, 2004.
16. P. Manadhata and J. M. Wing. An attack surface metric. Technical Report CMU-CS-05-155, School of Computer Science. Carnegie Mellon University, 2005.
17. P. K. Manadhata, et. al. An approach to measuring a systems attack surface. Technical Report CMU-CS-07-146, School of Computer Science. Carnegie Mellon University, 2007.
18. R. Mullen. The lognormal distribution of software failure rates: application to software reliability growth modeling. In *The Ninth International Symposium on Software Reliability Engineering*, pages 134 –142, nov. 1998.
19. R. Ortalo, et. al. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Transactions on Software Engineering*, 25(5):633–650, 1999.
20. J. Pamula, et. al. A weakest-adversary security metric for network configuration security analysis. In *QoP '06: Proceedings of the 2nd ACM workshop on Quality of protection*, pages 31–38, New York, NY, USA, 2006. ACM Press.
21. S. Schechter. How to buy better testing. In *Proceedings of the International Conference on Infrastructure Security (InfraSec'02)*, number 2437 in Lecture Notes in Computer Science, pages 73–87. Springer-Verlag, London, UK, 2002.
22. A. Stewart. On risk: perception and direction. *Computers & Security*, 23(5):362–370, 2004.
23. G. Stoneburner, et. al. Risk management guide for information technology systems. Technical Report 800-30, National Institute of Standards and Technology, 2001.
24. M. Swanson, et. al. Security metrics guide for information technology systems. Technical Report 800-55, National Institute of Standards and Technology, 2003.
25. R. B. Vaughn, et. al. 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.
26. L. Wang, et. al. 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, 2008. Springer-Verlag.
27. L. Wang, et. al. Minimum-cost network hardening using attack graphs. *Computer Communications*, 29(18):3812–3824, 2006.