Formal approach to security metrics. What does "more secure" mean for you?[*]

Leanid Krautsevich
Department of Computer Science
University of Pisa
Largo B. Pontecorvo 3, Pisa, Italy
krautsev@di.unipi.it

Fabio Martinelli
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche
G. Moruzzi 1, Pisa, Italy
fabio.martinelli@iit.cnr.it

Artsiom Yautsiukhin
Istituto di Informatica e Telematica
Consiglio Nazionale delle Ricerche
G. Moruzzi 1, Pisa, Italy
artsiom.yautsiukhin@iit.cnr.it

ABSTRACT

Security metrics are the tools for providing correct and up-to-date information about a state of security. This information is essential for managing security efficiently. Although a number of security metrics were proposed we still need reliable ways for assessment of security. First of all, we do not have a widely-accepted and unambiguous definition which defines what it means that one system is more secure than another one. Without this knowledge we cannot show that a metric really measures security. Second, there is no a universal formal model for all metrics which can be used for rigourous analysis. In this paper we investigate how we can define "more secure" relation and propose our basic formal model for a description and analysis of security metrics.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Miscellaneous—*Security*; K.6.4 [**Management of Computing and Information Systems**]: System Management—*Quality assurance*; D.2.8 [**Software Engineering**]: Metrics

General Terms

Security, Measurement, Management

Keywords

security metrics, formal metrics, security measurements

1. INTRODUCTION

More than ten years security community has been looking for the metrics which can measure security correctly and unambiguously. A number of different metrics have been proposed from specific ones, which measure a specific part of a system (e.g., time between antivirus updates), to general metrics, which assess security as a whole (e.g., attack surface) [8, 5]. Unfortunately, neither one metric nor a closed set of metrics are widely accepted for correct measurement of security as a whole and currently many of them are used simultaneously.

Such amount and diversity of metrics are caused by our inability to prove that a metric really measures security. One of the causes for this uncertainty is that there is no clear, unambiguous, and widely accepted definition of "more secure" relation. Every inventor of security metrics *defines* what "more secure" is by means of metrics, but *does not prove* that the metric really indicates changes in security.

For rigid proofs a formal description of metrics is required. Many authors state that there is a need for formal descriptions of security metrics [7, 23]. Such formalism, general for all metrics, must help to define metrics precisely, prove that metrics are the ones we need, and analyse how metrics relate to each other. Surely, there is a huge gap between theory and practice (e.g., see [7]). On the other hand, comparison of theoretical and practical versions of a metric should indicate the assumptions required for application of this metric.

In this article, we consider the problem of defining what "more secure" means and propose a small step forward in this direction. We propose a formal model which is capable of describing many of general security metrics. We used this model in order to analyse these metrics and consider relations between them. The proposed work is the first one to our knowledge which formally defines many different metrics and evaluates them from the correctness perspective. On the other hand, this work is only an initial step and we do not consider complex situations in this paper. The target of our analysis is just a system which is applied out of a context (i.e., we do not consider preferences of attackers and possible impact). We will add context in our model in the next version of our model.

The paper is organised as follows. Section 2 shows what metric means in theory of measurement and in the security community. Section 3 presents our basic formal model. In Section 4, we formally define several metrics and analyse them. We show what "more secure" means for different stakeholdes in Section 5. How a behaviour of attackers affects applicability metrics is analysed in Section 6. We conclude the paper with a discussion (Section 7), related work (Section 8), and a conclusion (Section 9).

[*]This work has been partially supported by EU-FP7-ICT CONSEQUENCE and EU-FP7-ICT CONNECT projects.

ECSA 2010 August 23-26, 2010, Copenhagen, Denmark
Copyright 2010 ACM 978-1-4503-0179-4/10/08 ...$10.00.

2. METRICS IN MATHEMATICS AND IN IT SECURITY

In the measurement theory, we can find the following theorem which helps to establish a link between an empirical evidence and an objective measurement. This is a central theorem which is called a representation theorem [21, 4]:

Definition 1 *Let Q be a set of elements and r and q be its members ($r, q \in Q$). Let also $\boldsymbol{R} = \{R_1, ..., R_n\}$ be a set of relations on Q. The tuple $\langle Q, \boldsymbol{R} \rangle$ is called an empirical relational system. Measurement can be seen as an objective-empirical function which assigns a real value to an element ($M : Q \mapsto \mathbb{R}$) and $\boldsymbol{P} = \{P_1, ..., P_n\}$ is a set of relations on $\mathbb{R}$ (reals) which is in a binary relation with $\boldsymbol{R}$ (i.e., each R_i corresponds to P_i). Then:*

$$\forall i \; R_i(r, q, ...) \Leftrightarrow P_i(M(r), M(q), ...) \tag{1}$$

For our purposes we simplify the representation theorem.

Definition 2 *We can say that a security measurement function is representative if one of the following relation holds*

$$\begin{aligned} \forall r, q \in Q \; (r \sim_S q) \Leftrightarrow M(r) = M(q) \; \mathit{and} \\ ((r \succ_S q) \Leftrightarrow M(r) > M(q) \; \mathit{xor} \\ (r \succ_S q) \Leftrightarrow M(r) < M(q)) \end{aligned} \tag{2}$$

where, $r \sim_S q$ means that r is equally secure as q, and $r \succ_S q$ means that r is more secure than q. Definition 2 shows that *a measurement function must be monotone.* The well-known definition of metrics in the measurement theory is [12]:

Definition 3 *Metric is a function M on a set Q which determines the distance between two members of the set ($M : Q \times Q \mapsto \mathbb{R}$) and satisfies the following properties:*

1. *$M(q_1, q_2) \geq 0 \; \forall q_1, q_2 \in Q$ (positivity)*
2. *$M(q_1, q_2) = 0$ iff $q_1 = q_2$. $\forall q_1, q_2 \in Q$ (identity)*
3. *$M(q_1, q_2) = M(q_2, q_1) \; \forall q_2, q_1 \in Q$ (symmetry)*
4. *$M(q_1, q_3) \leq M(q_1, q_2) + M(q_2, q_3) \; \forall q_1, q_2, q_3 \in Q$ (triangle inequality)*

Note, that Definition 3 already includes a measurement function: before defining the distance the mapping from empirical quantities to real numbers is established [1, 3].

The IT security community always uses the term "metric" as it is shown in Definition 2: one value is assigned to a system which defines how secure the system is. In the following, we stick to the common definition of "metric" accepted in the IT security community (i.e., Definition 2).

Challenge 1 *We must define what does it mean that two systems are equally secure or that one system is more secure than another one.*

These relations should be similar to the ones from physics where without measurements we often can say that one object is hotter/longer/brighter than another one. For example, the length of objects can be compared simply by putting the objects close one to another. Unfortunately, in the security community there is no such widely accepted answer. Usually, authors first define a way of measurement and then say that this means that the relation between two measurements defines relations between security levels of the two systems (e.g., [19]). In this paper, we will give a close look to this challenge.

3. BASIC FORMAL MODEL

We are going to consider Challenge 1 from a theoretical point of view. First, we define a formal model for a more accurate discussion about security strength and security metrics. We define security (similar to [17]) as follows:

Definition 4 *Let S be a system and X an attacker. A system and an attacker perform some actions ($a \in A$) and move from one state to another one. We denote a trace of actions completed by a system or an attacker as $\gamma \in \Gamma$. $\gamma' \bullet \gamma'_X$ 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[1] if and only if*

$$\begin{aligned} \forall X, \; \forall \gamma, \; S \xrightarrow{\gamma'} S' \; \wedge \; X \xrightarrow{\gamma'_X} X', \; \gamma = \gamma' \bullet \gamma'_X \\ S \| X \xrightarrow{\gamma} S' \| X' \Rightarrow P_{sec}(S' \| X') = \boldsymbol{F}(alse) \end{aligned} \tag{3}$$

We use the usual notation of the process algebra [17]. Function $P_{sec}(S' \| X')$ says if the system is compromised. We define an attacker X simply as a set of possible traces the attacker can launch against the system. We write $\gamma \in X$ 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: $\gamma = a_1 \circ a_2 \circ \cdots \circ a_n$.

Relaxing $\forall \gamma$ condition we can derive a simple definition that determines the 'more secure' relation.

Criterion 1 *Let $\mathcal{X}_A$ be a set of attackers relevant for system A, and $\mathcal{X}_B$ be a set of attackers relevant for system B. We say that system A is more secure than or equal to B ($A \succeq_S B$) if $\Gamma_A \subset \Gamma_B$, where:*

$$\begin{aligned} \Gamma_A = \{\gamma'_X \mid \gamma'_X \in X_A \in \mathcal{X}_A \; \gamma = \gamma' \bullet \gamma'_X \wedge \\ A \| X_A \xrightarrow{\gamma} A' \| X'_A \Rightarrow P_{sec}(A' \| X'_A) = \boldsymbol{T}\} \\ \Gamma_B = \{\gamma''_X \mid \gamma''_X \in X_B \in \mathcal{X}_B \; \hat{\gamma} = \gamma'' \bullet \gamma''_X \wedge \\ B \| X_B \xrightarrow{\hat{\gamma}} B' \| X'_B \Rightarrow P_{sec}(B' \| X'_B) = \boldsymbol{T}\} \end{aligned} \tag{4}$$

This security criterion says that if a set of possible attacks on one system is broader than a set of attacks on another one then the later system is more or (at least) equally secure than the former one. Since this criterion does not allow distinguishing between equal or higher security in case $\Gamma_A \subset \Gamma_B$ we call this criterion *non sensitive.* The *sensitive* criteria can be formalised in the following way:

Criterion 2 *We say that $A \succ_S B$ if $\Gamma_A \subset \Gamma_B$*

Criterion 3 *$A \sim_S B$ if $\Gamma_A \equiv \Gamma_B$*

Proposition 1 *If any attacker which can compromise A can compromise B as well, then $A \succeq_S B$.*

Proof We have that:

$$\begin{aligned} \forall X, \; \forall \gamma'_X \in X, \exists \gamma' \; . \; A \xrightarrow{\gamma'} A' \; \wedge \; X \xrightarrow{\gamma'_X} X' \\ A \| X \xrightarrow{\gamma' \bullet \gamma'_X} A' \| X' \Rightarrow P_{sec}(A' \| X') = \mathbf{T} \wedge \\ \exists \gamma'', \; B \xrightarrow{\gamma''} B' \; \wedge \; X \xrightarrow{\gamma'_X} X' \\ B \| X \xrightarrow{\gamma'' \bullet \gamma'_X} B' \| X' \Rightarrow P_{sec}(B' \| X') = \mathbf{T}\} \end{aligned} \tag{5}$$

[1] Note that not all the security properties can be stated as reachability ones, as, e.g., information flow ones. However, for the purpose of the paper, this is not a major limitation.

In other words, all possible attacks Γ_A are relevant for B as well ($\Gamma_A \subseteq \Gamma_B$). Therefore, according to Criterion 1 (or Criterion 2 and 3) $A \succeq_S B$. □

Though the criteria (Criterion 1 or Criterion 2) indicate that one system is more secure than the other one it is a rare case when the set of possible attacks for one system is completely included into the set of possible attacks for another system. In other words, this criterion gives us only a partial order, and, thus, we need a more fine-grained way for defining the 'more secure' relation.

4. FORMAL DEFINITIONS OF METRICS

In this section we consider several metrics which can be used for measuring security strength and show how the metrics are used for defining security criteria.

Number of attacks.

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

Definition 5 *Number of attacks (N_{att})*

$$\begin{aligned} &\forall X,\ \forall \gamma,\ S \xrightarrow{\gamma'} S' \ \wedge\ X \xrightarrow{\gamma'_X} X',\ \gamma = \gamma' \bullet \gamma'_X \\ &N_{att} = |\{\gamma'_X \mid S\|X \xrightarrow{\gamma} S'\|X' \Rightarrow P_{sec}(S'\|X') = \boldsymbol{T}\} \wedge \\ &\nexists \hat{\gamma}'_X \ .\ \gamma'_X = \gamma'_X \bullet \hat{\gamma}'_X \ S\|X \xrightarrow{\gamma' \bullet \hat{\gamma}'_X} S'\|X' \Rightarrow \\ &P_{sec}(S'\|X') = \boldsymbol{T}\}| \end{aligned} \tag{6}$$

The last line of Definition 5 leaves only the minimal sequences of attacks (i.e., only essential steps for an attack are considered). The security criterion is then defined as follows:

Criterion 4

$$A \succ_S B \ \textit{iff}\ N_{att}(A) < N_{att}(B) \tag{7}$$

Minimal cost of attack.

The idea behind this metric is that the less an attacker has to spend in order to successfully execute an attack the less secure the system is. We consider "cost" in a wide sense, i.e., a combination of everything that attacker must spend in order to successfully execute an attack (money, resources, time, effort, etc.).

In this article, we assume that the cost of attack is a composition of two costs: the cost of discovery that an attack is possible (i.e., discover a vulnerability) and the cost of execution of an attack (i.e., exploitation of this vulnerability).

Costs of attack, exploitation and discovery can be defined in the following way:

Definition 6 *Cost of attack (C_{att}).*

$$\begin{aligned} &\textit{If}\ \gamma = a'_1 \circ a'_2 \circ \cdots \circ a'_n; \\ &C_{exp}(\gamma) = C_{exp}(a'_1) \oplus C_{exp}(a'_2) \oplus \cdots \oplus C_{exp}(a'_n) \\ &C_d(\gamma) = C_d(a'_1) \oplus C_d(a'_2) \oplus \cdots \oplus C_d(a'_n) \\ &C_{att}(\gamma) = C_{exp}(\gamma) \oplus C_d(\gamma); \end{aligned} \tag{8}$$

where a is an action executed by an attacker and $C_{att}(a)$ is the cost the attacker has to pay to launch this action. Operator $\oplus$ applied to costs means that costs are summed up.

Definition 7 *Minimal cost of attack (C^{min}_{att}).*

$$\begin{aligned} &\forall X,\ \forall \gamma,\ S \xrightarrow{\gamma'} S' \ \wedge\ X \xrightarrow{\gamma'_X} X',\ \gamma = \gamma' \bullet \gamma'_X \\ &C^{min}_{att}(S) = min\{C_{att}(\gamma'_X) \mid S\|X \xrightarrow{\gamma' \bullet \gamma'_X} S'\|X' \Rightarrow \\ &P_{sec}(S'\|X') = \boldsymbol{T}\} \end{aligned} \tag{9}$$

Minimal costs of exploitation and discovery are also sometimes used as metrics for security.

Definition 8 *Minimal cost of attack (C^{min}_{att}).*

$$\begin{aligned} &\forall X,\ \forall \gamma,\ S \xrightarrow{\gamma'} S' \ \wedge\ X \xrightarrow{\gamma'_X} X',\ \gamma = \gamma' \bullet \gamma'_X \\ &C^{min}_{exp}(S) = min\{C_{exp}(\gamma'_X) \mid S\|X \xrightarrow{\gamma' \bullet \gamma'_X} S'\|X' \Rightarrow \\ &P_{sec}(S'\|X') = \boldsymbol{T}\} \\ &C^{min}_{d}(S) = min\{C_{d}(\gamma'_X) \mid S\|X \xrightarrow{\gamma' \bullet \gamma'_X} S'\|X' \Rightarrow \\ &P_{sec}(S'\|X') = \boldsymbol{T}\} \end{aligned} \tag{10}$$

The criterion is

Criterion 5

$$A \succ_S B \ \textit{iff}\ C^{min}_{att}(A) > C^{min}_{att}(B) \tag{11}$$

Minimal cost for reduction of attacks.

We can measure security by counting the cost required to update the system in order to achieve perfect security (similar to [25]). Of course, we would like to count only efficient investments in security and, thus, this cost must be minimal.

Definition 9 *Let some function Red improves the security strength of a system according to the amount of allowed investments. Then, the minimal cost of reduction of all attacks (C_{red}).*

$$\begin{aligned} &C_{red} = min\{C | S^* = Red(C,S)\ . \\ &\forall X,\ \forall \gamma,\ S^* \xrightarrow{\gamma'} S'^* \ \wedge\ X \xrightarrow{\gamma'_X} X',\ \gamma = \gamma' \bullet \gamma'_X \\ &S^*\|X \xrightarrow{\gamma} S'^*\|X' \Rightarrow P_{sec}(S'^*\|X') = \boldsymbol{F}\} \end{aligned} \tag{12}$$

The criterion is

Criterion 6

$$A \succ_S B \ \textit{iff}\ C_{red}(A) < C_{red}(B) \tag{13}$$

Shortest Length of Attacks.

An intuition behind this metric is the following: the less steps an attacker has to make, the simpler is to execute the attack successfully, and the less secure the system is [18].

Definition 10 *First we define the length of attacks as:*

$$\begin{aligned} &L(\gamma) = |\gamma| = n\ \textit{where} \\ &\gamma = a_1 \circ a_2 \circ \cdots \circ a_n \end{aligned} \tag{14}$$

Now we can easily define the shortest attack as:

$$L^{min}(S) = min\{L(\gamma'_X) \mid S\|X \xrightarrow{\gamma'\bullet\gamma'_X} S'\|X' \Rightarrow P_{sec}(S'\|X') = \boldsymbol{T}\} \quad (15)$$

The criterion is

Criterion 7

$$A \succ_S B \textit{ iff } L^{min}(A) > L^{min}(B) \quad (16)$$

Maximal probability of attack.

The probability to accomplish an attack successfully is a well-known metric. The metric defines how probable is that an attacker is capable of reaching its final goal.

Definition 11

We define maximal probability of attack as follows:

$$\textit{If } \gamma = a'_1 \circ a'_2 \circ \cdots \circ a'_n;$$
$$p(\gamma) = p(a'_1) \otimes p(a'_2) \otimes \cdots \otimes p(a'_n)$$
$$P^{max}(S) = max\{p(\gamma'_X) \mid S\|X \xrightarrow{\gamma'\bullet\gamma'_X} S'\|X' \Rightarrow P_{sec}(S'\|X') = \boldsymbol{T}\} \quad (17)$$

Operator $\otimes$ in this case means a multiplication of probabilities. In other words, in order to get the probability to execute an attack successfully every action required for the attack must be successfully accomplished.

Now, the security criterion can be transformed into the following one:

Criterion 8

$$A \succ_S B \textit{ iff } P^{max}(A) < P^{max}(B) \quad (18)$$

Overall probability of success.

Defining security strength using the maximal probability of attack is not very descriptive. In particular, elimination of possible attacks, except the most probable one, does not change the overall strength of security. Therefore, we provide another definition based on probability. The value we get can be seen as a probability that an attacker executing all attacks one-by-one is not able to compromise the system:

Definition 12

We define probability of success as follows:

$$\textit{If } p(\gamma) = p(a'_1) \otimes p(a'_2) \otimes \cdots \otimes p(a'_n)$$
$$P^{suc}(S) = \oplus_{\forall i} p(\gamma'_{X,i}) = 1 - \prod_{\forall i}(1 - p(\gamma'_{X,i}))$$
$$\textit{where } \forall\gamma'_{X,i}, \exists\gamma' \ . \ S\|X \xrightarrow{\gamma'\bullet\gamma'_{X,i}} S'\|X' \Rightarrow P_{sec}(S'\|X') = \boldsymbol{T}\} \quad (19)$$

This metric is sensitive to any changes in security. The security criterion in this case is the following:

Criterion 9

$$A \succ_S B \textit{ iff } P^{suc}(A) < P^{suc}(B) \quad (20)$$

One more probabilistic metric is usually used for measuring security: the average probability to compromise a system. In order to compute this metric we need to know which attack is more frequent than another one. This knowledge depends on the context where the system is implemented and, thus, we cannot formalise this metric at this stage (but we will use this metric in the future).

Attack surface metric.

This metric has been proposed by M. Howard and J. Wing [6, 14]. We generalised the methodology proposed in [14] and adapted it for our model. We define the attack surface metric as follows.

Definition 13 *Let a set of actions which can be done by a system be $A_S = \{a \mid a \in \gamma \in S\}$. Let a set of resources which can be used after an action can be found with the following function: $Res : A \mapsto 2^{\mathrm{RES}}$, where* RES *is a set of all possible resources. If we have a set of actions A we can find all types for the resources used and achievable by these actions: $Type\_Set = \{t \mid \exists a \in A \ . \ Res(a) \in t \in \mathrm{TYPE}\}$, where* TYPE *is a set of all possible types. We also need a function which selects the subtypes of resource types which satisfy some properties: $Prop : 2^{\mathrm{PROP}} \circ 2^{\mathrm{TYPE}} \mapsto 2^{\mathrm{TYPE}}$. Lets call Attack_Class a set of subtypes satisfying some property: $Attack\_Class = Prop(\mathrm{PROP} * Type\_Set)$. Finally, if k indicates a specific attack class and w_k is a weight assigned to the k-th attack class then the attack surface metric can be defined:*

$$ASM^w = \sum_{\forall k}(|R(Attack\_Class_k)| * w_k), \ \textit{where}$$
$$R(Attack\_Class_k) = \{Res(a) \mid \exists a \in A_S \ \wedge$$
$$Res(a) \in Attack\_Class_k \ \wedge \ A_S = \{a \mid a \in \gamma \in S\}\} \quad (21)$$

In the set of considered resources (RES), types (TYPE) and properties (PROP) are defined by analysts. In order to remove this human-based factor we assume that there are the corresponding universal sets which contain all possible units of the required kind.

Criterion 10

$$A \succ_S B \textit{ iff } ASM^w(A) < ASM^w(B) \quad (22)$$

The last remark about this metric we want to make is that the metric was significantly improved in the further work [15, 16]. We do not consider the latest version of the metric because this version considers the system applied in a specific context when we consider systems out of a context.

Percentage of compliance.

Percentage of compliance[10, 9] with some standard, a guideline or a check list of other kind can be formalised in the following way.

Definition 14 *Check list is a simple set of actions of a system: $\Gamma^{cl} \subseteq \Gamma$. Let a set of satisfied items in the list be $\Gamma^S = \{\gamma | \gamma \in S \ \wedge \ \gamma \in \Gamma^{cl}\}$. The the metric is:*

$$CLM = |\Gamma^S|/|\Gamma^{cl}| \quad (23)$$

A weighted check list ration can be seen as follows:

$$CLM^w = \sum_{\gamma_i \in \Gamma^S} w_i * |\gamma_i|/|\Gamma^{cl}| \quad (24)$$

Criterion 11

$$A \succ_S B \text{ iff } CLM(A) > CLM(B) \text{ or}$$
$$A \succ_S B \text{ iff } CLM^w(A) > CLM^w(B) \qquad (25)$$

4.1 Evaluation of metrics

We evaluate the formalised metrics against the security Criteria 1 and 2. The sketches of proofs can be found in Appendix A and the result is shown in Table 1. Note, that both metrics which fail to satisfy our criteria still can be useful (e.g., percentage of compliance can be used as an indicator that the system satisfies some set of requirements to some extent) but assessing security strength both metrics rely on very strong assumptions. Moreover, we remind that satisfaction of the criteria (sensitive or non-sensitive) does not guarantee that a metric really measures security. We can only say that the metric *may* be the one which is good for such measurement.

N_{att}	C_{att}^{min}	C_{red}	L^{min}	P^{max}	P^{suc}	ASM^w	CLM
s	n-s	n-s	n-s	n-s	s	no	no

Table 1: Results of satisfaction of security criteria. "s"- sensitive, "n-s" - non-sensitive, "no" - fails both criteria.

Another analysis of metrics we made is checking metrics for their equivalence, i.e., if metrics perform the same measurement but use different scales. For our purpose, we should check if metrics are monotone [21, 4].

Definition 15 *Two security metrics are scalable (or unique) up to some transformation f if:*

$$M(r) > M(q) \Leftrightarrow f(M(r)) > f(M(q)) \text{ or}$$
$$M(r) > M(q) \Leftrightarrow f(M(r)) < f(M(q)) \qquad (26)$$

Note, that Definition 15 allows us only to preserve the order. We analysed security metrics from Section 4 and found that all of them are independent ("X" in Table 2). On the other hand, we found that some metrics can be derived from others with some (often, very strong) assumptions ("?X"). For example, maximal probability can be found as $P^{max}(S) = p^{L^{min}(S)}$ if every action has the same probability of success. The brief intuition about the dependencies presented in Table 2 can be found in Appendix B.

5. METRICS AND STAKEHOLDERS

Using only Criterion 1 or 2, we cannot decide which metric is more appropriate for measuring security. Such decision cannot be done because the criterion we use is too coarse (we can apply only a partial order to compare systems) and, thus, we need other criteria to make a more fine grained analysis of metrics or, ideally, an unambiguous definition of "more secure". Therefore, currently we have to accept that several metrics can be used. The selection of more appropriate metric can be done depending on who needs this metric.

Various metrics are useful for different stakeholders. A security team or administrators are more interested in what has to be done to reduce amount of penetrations. Thus, a number of possible attacks is more useful for these stakeholders. Also attack surface can be useful too to see how assets can be better protected.

	N_{att}	C_{att}^{min}	C_{red}	L^{min}	P^{max}	P^{suc}	ASM^w	CLM
N_{att}	▨	X	?X	X	X	?X	X	X
C_{att}^{min}	X	▨	X	?X	X	X	X	X
C_{red}	?X	X	▨	X	X	X	X	X
L^{min}	X	?X	X	▨	?X	X	X	X
P^{max}	X	X	X	?X	▨	X	X	X
P^{suc}	?X	X	X	X	X	▨	X	X
ASM^w	X	X	X	X	X	X	▨	X
CLM	X	X	X	X	X	X	X	▨

Table 2: Relations between metrics.

Cost of reduction gives information for those who are responsible for a security budget (e.g., security managers and financial managers). This metric can be useful when more investments in security are required.

Minimal cost of attack, probabilities and length of attacks are more useful for the analysts studying attackers. After an analysis these metrics can be provided to security staff which can improve the system knowing the weakest places. Of course, these values are interesting for an attacker, who wants to conduct its attack in the most efficient way.

Percentage of compliance is a metric for managers who have to be sure that the security of the system complies with some guidelines or laws. The analysis shows that adding more suggested security controls does not obligatory increases the security level, because the suggested controls are not specified for the needs of a concrete system.

6. ATTACKER MODELS AND METRICS

One side conclusions we made out of our work, is that a definition of security depends on behaviour of an attacker.

Considering security strength, even not in a specific context, we take into account possible behaviour of an attacker. For example, we say that a castle with thicker walls is more secure than the one with thinner walls. In this case, we implicitly assume that an attacker is going to break the walls with cannons or catapults. Definition 1 already takes into account all possible ways which an attacker can follow to break the system. On the other hand, the definition does not consider *how* the attacker is going to select an attack to execute among several alternatives and does not say what kind of knowledge the attacker possesses. In the following, we are going to show that this moment has a crucial effect on selection of security metrics.

We are going to consider two simple models of an attacker in order to show how different metrics react on behaviour of these attackers.

Omniscient attacker.

This is a "worst-case attacker". The attacker has a complete knowledge of the system: knows all possible attacks, costs he has to pay to execute each attack and also the probability that an attack will be successful. With all this knowledge the attacker will always select the "easiest" way (less costly or more probable[2]). Thus, the existence of other attacks rather than the "easiest" one does not affect the overall security strength because these attacks will never be used. In this case, such metrics as minimal cost of attack or the most probable attack are the most appropriate choice.

Although such attacker is popular in the literature it is not suitable for estimation of a real security strength, the property which security metrics do have to measure. If such attackers were possible all attacks on the same system would be the same. On the contrary, we see the diversity of attacks (see, for example, the experiment described by E. Jonsson and T. Olovsson [11]).

Blind attacker.

This attacker is another extreme: the attacker does not know anything about the system. The attacker finds the first possible attack and tries to execute it because there is no knowledge of how easy the attack is. In other words, the attacker selects attacks randomly. With such an attacker in mind every attack will contribute to the overall security strength, but not only the "easiest" one. Therefore, metrics like minimal cost of attacks are not appropriate for estimation of security strength, because they do not register improvement of security strength caused by hardening of other attacks, except the "easiest" one.

Of course, neither the first nor the second model are good for description of the behaviour of attacker, since an attacker always has some knowledge about the system, but this knowledge is not complete. Therefore, new and more realistic models of an attacker are required. On the other hand, two extreme models already presented illustrate that different conclusions can be derived with respect to the considered behaviour of an attacker.

7. DISCUSSION

In this paper, we have presented our basic model for describing security metrics in a formal way. All metrics we have selected are the ones which measure security out of a context. We are aware that 'a "good metric" should also ideally be context specific' [8], but we see this paper as an initial step which have to be done before a more complex situation is considered. For example, in this article we were not able to consider average probability of success since for this purpose we need the information about attractiveness of one attack in a comparison with another one (threat, in short). Another important example of application of a system in a specific context is possible damage for the organisation. For example, threats and possible damage are required for modelling of risk [20, 2] or a new version of attack surface [15, 16].

In Section 3, we provided a simple empirical criterion for partial analysis of security metrics. As we see from the article this criteria is not enough because many metrics satisfy it. Therefore, we either need to find more empirical criteria for a more fine-grained analysis or, ideally, define what we mean by "more secure". Note, that we do not claim that the metrics which do not satisfy our criterion are bad. We only say that we cannot rely on them entirely when we consider security of a system.

We have found that cost of attacks, probability of attacks and skills of attackers are not entirely independent. Unfortunately, we are not aware about a study which formally defines the relation between these attributes. Thus, we used an oversimplified model. The only work we are aware of was done by E. Jonsson and T. Olovsson [11], but the study is empirical and provides only approximate dependency.

8. RELATED WORK

We already pointed out that in the security community there is no agreement on what to consider a good metric for security of a system. A. Wang [23] restated four axioms proposed for measuring the complexity of programs in order to create axioms for security metrics. These axioms are either too simple, i.e., all metrics satisfy them (e.g., "the measure must not assign the same number to all systems") or unclear, what do they mean in a context of security and their validity is arguable (e.g., "the measure must be sensitive to the ordering of the system components").

Approaches based on attack graphs are close to our work. First of all, these approaches are also based on the idea to model behaviour of an attacker as a sequence of steps (exploiting vulnerabilities). Secondly, these approaches are also based on a formal description of a system. Furthermore, the authors also use various metrics for evaluation of a system: probability of successful attack [24], minimal cost of attack [19], minimal cost of reduction [25], shortest path [18]. Due to the different models our formal descriptions are different. Moreover, some of the metrics are defined differently (e.g., minimal cost of attack [19]) and their description is not completely formal, but the metrics are of the same kind anyway. Despite the similarities, our work has a different goal - to *analyse* different metrics and relations between them. Moreover, we aim to prove which metric is more appropriate for measuring security, while the authors of papers on attack graphs just define these metrics to measure security strength.

P. Manadhata and J. M. Wing in their work also provided a formal model for defining attack surface metric[14, 15, 16]. In contrast to our work, the model provided by these authors is more focused on the resources which can be compromised (because of nature of the proposed metric) rather than on the ways how an attack can be conducted. Even a new, more advanced model [15, 16] does not explicitly show how an attacker can compromise a system, but assumes that this is possible if there is a way to access the resource. Similar to attack graph approaches, this formal model is made to work with a specific metric: attack surface metric, when our goal is to analyse different metrics.

Another example of the metric which has been formally defined is a "mean time to security failure" metric was proposed by Madan et al. [13]. The model is aimed to model behaviour of a system for a single-step attack, when we consider more complex scenarios.

M. Walter and C. Trinitis [22] have provided a formal model for describing security of a system. The authors consider a system as a castle where several ways (doors) to penetrate into the caste exist. Probability of penetration through a door is used to compute the overall security of a castle (system). In fact, the work is similar to attack graph approaches (if we consider vulnerabilities as doors).

9. CONCLUSION AND FUTURE WORK

[2] We analyse a system using cost and probability separately. See Section 7

In this paper, we have presented our initial model of a formal description and analysis of security metrics. First of all, we have shown that in theory of measurement term "metric" has a different meaning (distance) than the one usually used in the security community. We have formalised a number of security metrics which can be found in the literature and evaluated them against a very simple empirical criteria. We also investigated dependencies among metrics and found that in a strict sense all metrics are independent, but there are some correlations between these metrics. One of the main conclusions we have made out of our research is that we do not have a strict empirical notion of "more secure" and, therefore, we cannot say which metric is good (or bad) for measuring security. Without this relation we can only say that security metrics should be used depending on the entity which requires evaluation of security, i.e., a stakeholder. Another conclusion we can draw out of our work is that a metric can be considered good or bad depending on the model of an attacker.

In the future, we are going to improve our model and take into account also the context in which a system is installed (e.g., assets which are protected, possible threats, etc.). Another direction is to find more fine-grained criteria for "more-secure" relation. For example, we are going to give a closer look on amount of possible penetrations, taking into account different behaviour of attackers. Finally, we would like to investigate relations between probability of successful attack, cost of attack and skills of an attacker.

10. REFERENCES

[1] J. Barzilai. Measurement and preference function modelling. *International Transactions in Operational Research*, 12:173–183, 2005.

[2] S. A. Butler. Security attribute evaluation method: a cost-benefit approach. In *Proc. of ICSE-02*, pages 232–240. ACM Press, 2002.

[3] E. Coatanea et al. Measurement theory and dimensional analysis: methodological impact on the comparison and evaluation process. In *Proc. of ASME-07*, 2007.

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

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

[6] M. Howard, J. Pincus, and J. Wing. Measuring relative attack surfaces. Technical Report CMU-TR-03-169, CMU, 2003.

[7] W. Jansen. Directions in security metric research. Technical Report NISTIR 7564, NIST, 2009.

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

[9] E. Johansson and P. Johnson. Assessment of enterprise information security - an architecture theory diagram definition. In *Proc. of CSER-05*, 2005.

[10] E. Johansson and P. Johnson. Assessment of enterprise information security - estimating the credibility of the results. In *Proc. of SREIS-05*, 2005.

[11] E. Jonsson and T. Olovsson. A quantitative model of the security intrusion process based on attacker behavior. *IEEE TSE*, 23(4):235–245, 1997.

[12] I. Kramosil, and Jiri Michalek. Fuzzy metrics and statistical metric spaces. *Kybernetica*, 11(5):336–344, 1974.

[13] B. B. Madan, et al. A method for modeling and quantifying the security attributes of intrusion tolerant systems. *Performance evaluatin journal*, 1-4(56):167–186, 2004.

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

[15] P. Manadhata and J. M. Wing. An attack surface metric. Technical Report CMU-CS-05-155, CMU, 2005.

[16] P. K. Manadhata, et al. An approach to measuring a system's attack surface. Technical report CMU-CS-07-146, CMU, 2007.

[17] F. Martinelli. Analysis of security protocols as open systems. *TCS*, 290(1):1057–1106, 2003.

[18] R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE TSE*, 25(5):633–650, 1999.

[19] J. Pamula, et al. A weakest-adversary security metric for network configuration security analysis. In *Proc. of QoP-06*, 2006. ACM Press.

[20] G. Stoneburner, A. Goguen, and A. Feringa. Risk management guide for information technology systems. Technical Report 800-30, NIST, 2001.

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

[22] M. Walter and C. Trinitis. Quantifying the security of composed systems. In *Proc. of PPAM-05*, 2005.

[23] A. J. A. Wang. Information security models and metrics. In *Proc. of ACM-SE-05*, pages 178–184, USA, 2005. ACM Press.

[24] L. Wang, et al. An attack graph-based probabilistic security metric. In *Proc. of DBSec-09*, 2008. Springer-Verlag.

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

APPENDIX

A. PROOFS FOR SECURITY CRITERIA

Proof For *number of attack* metric from relation $\Gamma_A \subset \Gamma_B$ we can deduce that $N_{att}(A) < N_{att}(B)$ ($|\Gamma_A| = N_{att}(A)$). This is exactly what Criterion 4 states.

For *minimal cost of attack* we can divide Γ_B in two sets: $\Gamma_B = \Gamma_A \cup \Gamma'_B$. $\Gamma'_B \cap \Gamma_A = \emptyset$. Thus, the cheapest attack is either in Γ_A or in Γ'_B. If the cheapest attack is in Γ_A then we have that $CostAt(A) = CostAt(B)$. If the cheapest attack belongs to Γ'_B then $CostAt(A) > CostAt(B)$.

The proofs for *minimal cost of reduction*, *maximal probability of attack* and *minimal length of attack* metrics are the same as for *minimal cost of attack* metric, because the minimal or the maximal value of B is either in Γ_A or in Γ'_B.

We again divide Γ_B in two sets: $\Gamma_B = \Gamma_A \cup \Gamma'_B$. $\Gamma'_B \cap \Gamma_A = \emptyset$ in order to prove the satisfaction of the criteria for *overall* *probability of success* metric. The metric for system A is computed as follows: $P^{suc}(A) = 1 - \prod_{\forall i}(1 - p(\gamma_i))$. Thus, we can define $P^{suc}(B)$ through $P^{suc}(A)$: $1 - P^{suc}(B) = (1 - P^{suc}(A)) * \prod_{\forall \gamma_j \in \Gamma'_B}(1 - p(\gamma_j))$. Since the probabilities are always less than 1 we can deduce the following inequality: $1 - P^{suc}(B) < (1 - P^{suc}(A))$. Thus, $P^{suc}(B) > P^{suc}(A)$.

Attack surface metric. Consider that reaching a resource by an attacker means to compromise the system. The main problem if this metric is that it considers only the last step (which denotes that the resource can be reached by an attacker: $Res(a) \in Attack\_Class$). Moreover, the authors also assume that if there is a legal way to use a resource then there is also a way for an attacker to reach the resource. Assume that the later observation holds. Now, if we consider A and B which have the same set of resources, which belong to the same sets of attack classes. More ways to compromise B do not contribute to the attack surface value for B in this case. In contrary, we can remove one of the resources from B to which no sequences of actions available for an attacker (attacks) and this makes $ASM(A) > ASM(B)$ while $\Gamma_A \subset \Gamma_B$. Note, that we use the version of the metric presented in [14] (a new version [15, 16] partially solves the problem).

Percentage of compliance metric is more oriented to how a system behaves rather than what an attacker can do. Naturally, there is a correspondence between security actions and possibility for an attacker to compromise the system, but not all requirements inserted into a check list are relevant for the system. Therefore, the two systems which implemented the same set of requirements have the same values of the metrics, even if they have different sets of attacks, e.g., $\Gamma_A \subset \Gamma_B$. Now, if we add an additional implementation of a requirement from a check list to the system B, which though does not remove any possible attack, we have that $ASM^w(A) < ASM^w(B)$. □

B. SCALABILITY OF METRICS

In this part of the Appendix, we give only an intuition which indicates that Definition 15 does not hold for a pairs of metrics, due to the lack of space. In this section, we only show that most metrics cannot be seen simply as a monotone function from another metric and we indicate the assumptions with which such monotone function can be found.

Number of attacks.

Two systems with different sets of attacks will have different qualities of attacks: different minimal costs, different maximal probabilities, different length of attacks, different cost of reduction of attacks. By the same reason, the overall probability of success can be greater for the system with lower number of easiest attack than the one with higher number of hard attack. On the other hand, if the probability to execute every attack is the same (p) then the system with a lower number of attacks has a lower value of the metric (and $P^{suc}(S) = 1 - (1-p)^{N_{att}(S)}$. Also, if we assume that reduction of one attack does not depend on reduction of another one and has the same cost c then we can define cost of reduction as: $C_{red}(S) = c * N_{att}(S)$. A number of ways to reach valuable resources (compromise a system) do not depend on the number of the resources themselves (in strict sense). Also a greater set of security practices applied in one system do not guarantee that the system has less attacks.

Minimal cost of attack.

Increasing the amount of attacks with expensive attacks we can significantly variate the minimum cost of reduction and the overall probability of success metrics leaving the minimal cost of attack the same. In this paper, we consider the probability of an action to be independent from the cost of the action (though we agree that a more complex dependency model must be found). In general an attack with some length may have any cost. On the other hand, if we assume that every action has the same cost c then $C^{min}_{att}(S) = c * L^{min}(S)$. Adding or removing a resource to/from the system does not change the minimal cost of attack (unless we remove the goal of the attack with minimal cost). Similarly, adding or removing an applied security practice does not affect the minimal cost of attack.

Maximal probability of attack.

Increasing the amount of attacks with expensive attacks we can significantly variate the minimum cost of reduction and overall probability of success metrics leaving the maximal probability of attack the same. In fact a trace of very probable actions can be longer than a shorter trace with very difficult actions. On the other hand, if we assume that probability to execute any action is p then $P^{max}(S) = p^{L^{min}(S)}$. Similar to the minimal cost of attack adding or removing a resource to/from the system does not change the maximal probability of attack, neither adding or removing an applied security practice does.

Shortest length of attack.

Increasing the amount of attacks with expensive attacks we can significantly variate the minimum cost of reduction and overall probability of success metrics leaving the shortest length of attack the same. Similar to the minimal cost of attack adding or removing a resource to/from the system does not change the shortest length of attack, neither adding nor removing an applied security practice does.

Minimal cost of reduction.

Imagine that we have two systems with the same values of the minimal cost of reduction and the maximal probability of attack. Now if we remove the most probable attack from one system and the most expensive in reduction attack from another system we have that the first system is less probably will be compromised when the second is has smaller the minimal cost of reduction. But we have a reverse situation when we remove the less probable and the less expensive attacks. Removing an attack does not change the number of reachable resources. Also if we remove an attack by a countermeasure not listed in a check list the percentage of compliance with the check list will be the same.

Overall probability of success.

Since removing or adding an attack does not change a set of reachable resources than the overall probability of success and attack surface metrics are independent. With the same amount of applied countermeasures we can close the most probable attacks and the less probable.

Attack surface.

Adding or removing a countermeasure does not change the amount of resources in a system.