electronics

MDPI

Article

Construction and Analysis of Integral User-Oriented Trustworthiness Metrics

Evgenia Novikova *, Elena Doynikova *, Diana Gaifulina and Igor Kotenko *

St. Petersburg Federal Research Center of the Russian Academy of Sciences (SPC RAS), 14ya Liniya V.O. 39, 199178 St. Petersburg, Russia; gaifulina@comsec.spb.ru

* Correspondence: novikova@comsec.spb.ru (E.N.); doynikova@comsec.spb.ru (E.D.); ivkote@comsec.spb.ru (I.K.)

Abstract: Trustworthiness metrics help users to understand information system's or a device's security, safety, privacy, resilience, and reliability level. These metrics have different types and natures. The challenge consists of the integration of these metrics into one clear, scalable, sensitive, and reasonable metric representing overall trustworthiness level, useful for understanding if the users can trust the system or for the comparison of the devices and information systems. In this research, the authors propose a novel algorithm for calculation of an integral trustworthiness risk score that is scalable to any number of metrics, considers their criticality, and does not perform averaging in a case when all metrics are of equal importance. The obtained trustworthiness risk score could be further transformed to trustworthiness level. The authors analyze the resulting integral metric sensitivity and demonstrate its advantages on the series of experiments.

Keywords: trustworthiness; risk score; information security; privacy; integral metrics; calculation; sensitivity analysis; algorithm

Citation: Novikova, E.; Doynikova, E.; Gaifulina, D.; Kotenko, I. Construction and Analysis of Integral User-Oriented Trustworthiness Metrics. *Electronics* **2022**, *11*, 234. https://doi.org/10.3390/electronics11020234

Academic Editor: Krzysztof Szczypiorski

Received: 16 November 2021
Accepted: 5 January 2022
Published: 12 January 2022

1. Introduction

Trustworthiness metrics help users and security experts to understand an information system's or device security's safety, privacy, resilience, and reliability level, monitor it, check compliance to the information security and privacy standards, and make reasonable decisions. These metrics have different types and natures. The trustworthiness metric calculated based on the five aforementioned types of metrics can help users understand if they can trust the system and compare different systems and devices in terms of trust or comparing the system trustworthiness level in different time moments. The challenge consists of the integration of these metrics in one clear, scalable, sensitive, and reasonable metric.

While the authors consider the integration of different types of risk aware metrics on the example of the trustworthiness risk score, the challenge exists for the other integral metrics as well, for example, in the information security area, there is an integral risk score metric and countermeasure selection index that is usually calculated based on countermeasure efficiency for the security risk mitigation and countermeasure costs.

The researchers have proposed different approaches to overcome this challenge. The rather common approach is a table-based approach that is used mostly for nominal parameters. The first row and column of such table contain possible values of input metrics, while the inner cells of the table contain values of an integral score. For example, this approach is used within the facilitated risk analysis and assessment process (FRAAP) proposed in [1]. An obvious benefit of such an approach is the transparency of the calculation procedure; however, creating tables for more than three metrics is a quite complicated process. The min–max approach is usually used in the context of security measures selection and supposes minimization of parameters such as attack probability, attack impact, response costs, and maximization of parameters such as benefit from security measures implementation [2].

The approach based on weighted sum is also widely used, for example, it is adopted for calculating Common Vulnerability Scoring System (CVSS) metrics [3]. Application of the weighted sum requires setting ranks or weights for the metrics. In some cases, the definition of metrics weights is a quite natural process, and in other cases, it is a rather complicated task to set up the weights in such a way that they do not result in metric value averaging when all metrics are of equal importance.

The *motivation* of the paper is as follows. Nowadays, the trust-related metrics of the devices and systems become essential for the end-user. In many business scenarios that involve sensitive or/and confidential data processing, trust is one of the most critical features that should be provided by the information system. The end-user does not need the detailed telemetry that is essential for the security experts but needs a clear and objective metric for the comparison of the devices and systems.

For example, in Sweden, the forest mainly belongs to the private parties, and in order to coordinate their activities in terms of forest maintenance and protection against insect attacks and other illnesses, the government forestry agency requires obtaining sensitive and confidential data from different data owners [4]. To support this process the agency needs to provide a system the data owners could trust. Trust is based on components such as data confidentiality, integrity, and availability (CIA), privacy, resiliency, safety, and reliability. In many tasks, it is required to calculate these metrics separately, but for the end-users in the considered case, it is important to understand these metrics as an integral one—trust—to be able to understand integral risks.

The main *contribution* of the paper consists of developing the algorithm for integral trustworthiness risk score calculation and the series of experiments demonstrating the resulting integral metric sensitivity. The proposed algorithm is applicable for other types of integral risk-aware metrics as well.

The *novelty* of the proposed algorithm consists of the outlining of the integral risk score and an additive coefficient that increases the base value. The risk score base is the metric with the highest risk score or with the highest criticality, if such data are available. The additive coefficient considers the weights, current values, and possible maximum values of other metrics. The authors suggest applying a nonlinear logarithm function to calculate it. Unlike the weighted sum, it allows avoiding the averaging of the resulting value.

The paper is organized as follows. Section 2 analyzes the related research in the area. Section 3 specifies the requirements for integral trustworthiness metric calculation and introduces the algorithms for calculating integral metrics. Section 4 presents the sensitivity analysis of the proposed algorithms. Section 5 describes the conducted experiments and their results and provides the discussion. Section 6 contains the conclusion.

2. Related Research

Trustworthiness is essential for various areas of information technology. For example, in software design and development, it represents the software quality and considers the software attributes [5,6]. In cyber security awareness, the trustworthiness metric incorporates security, safety, privacy, resilience, and reliability metrics. Each of these metrics can be used separately, depending on the user's or security expert's goal, and should be calculated based on other more low-level metrics. The main feature of the integral trustworthiness metric in this case is that it incorporates metrics of a different nature.

A metric refers to the result of the analysis of two or more measurements taken over time [7]. Depending on the metric, different analysis models can be used to aggregate the measurements. While for the experts it is essential to obtain and analyze all these measurements, there are tasks where the integral metrics are used. For example, in the information security area, there is security monitoring and improvement, security decision support, etc. Besides, for the end-user who decides whether to trust the system or which device to choose, the integral objective and a clear score are required.

To obtain an integral security metric, it is required to aggregate metrics of a different nature. For this goal, different approaches can be used.

Security metrics assess such security functions as identification, protection, detection, responding, recovering, and accomplishment of security objectives such as confidentiality, integrity, availability, and accountability [8]. Security metrics are widely used for security strategic support, quality assurance, tactical and operational oversight, security monitoring and improvement, assessing the adequacy of in-place security controls, policies, and procedures, and consequently deciding on security investments, decision making, risk identification, risk management, and identifying priorities [9,10]. They incorporate or are closely connected with other types of metrics such as risk metrics, resilience metrics, authenticity metrics, privacy metrics, trustworthiness, countermeasure selection metrics, etc.

As it is mentioned in the Introduction, the rather common approach is table based. Its application for obtaining an integral security risk metric is described in the ISO/IEC 27005 standard [11] and within the FRAAP [1]. Its advantage consists in the transparency of the calculation procedure. Its main disadvantage consists in the fact that creating tables for more than three metrics is a quite complicated process.

The min–max approach is usually used in the context of security risk level representation and security measures selection, and supposes minimization of parameters such as attack probability, attack impact, response costs, and maximization of parameters such as benefit from security measures implementation [2]. For example, the metric Network Risk Distribution Degree (NRDD) representing the security risk level based on such approach is proposed in [12]. This metric increases if the risk for the important equipment in the network increases and indicates that the security policies for the important equipment should be adjusted.

In [13,14], the CVSS-based risk metric is proposed that supposes minimization of the maximum impacts and probabilities of attack for the computer network resources. Another example is the Return On Response Investment (RORI) index proposed in [15]. It increases if annual loss expectation and risk mitigation increase while annual infrastructure value and annual response cost decrease. It allows selecting the optimal countermeasures by maximizing the RORI index. In [16], a model for maximizing the benefit from investments to protect information is considered. In [17], the Return On Investment metric is used that maximizes benefit and minimizes costs of the investments.

The approach based on weighted sum is also widely used. One of the most representative examples is the integral metric for scoring the vulnerabilities' severity—CVSS score [3]. Application of the weighted sum requires setting ranks or weights for the metrics. In the case of the CVSS, the weights are the result of thorough statistical analysis and tuning. Another example is the integral metric for scoring the weaknesses' severity—CWSS score [18]. In [19,20], the weighted sum is used for the trustworthiness calculation. In [21], the weighted sum is considered for the trustworthiness calculation, but it is also mentioned that this approach can be misleading [22].

There are many studies related to trust and trustworthiness calculation [23–25]. For example, in [25], authors discuss the problem of calculating a trust based on sequential security measurements. This algorithm is based on the evaluation of a probability of a malicious act with a predefined error in the measurement. Trust is calculated as a composition of such measurements.

In this research, the authors propose a novel algorithm for an integral trustworthiness metric calculation that is scalable to any number of metrics, considers their criticality, and does not perform averaging in a case when all metrics are of equal importance. The authors consider the last feature as an essential one as soon as averaging can result in missing the trustworthiness gap.

3. Algorithm for Integral Trustworthiness Metric Calculation

When designing the algorithm, we analyzed existing approaches for calculation of the integral risk scores as well as approaches for measuring the trustworthiness of the

information systems and the metrics composing it and found out that integral metrics are usually based on more than two metrics [2,12,15].

This allowed us to identify the following requirements for the algorithm, calculating the integral risk score for a set of risk aware metrics.

- Requirement 1. Scalability. The algorithm should be scalable to a set of metrics, as recently developed trustworthiness measuring systems analyze different aspects of information systems such as security, safety, privacy, resilience, and reliability.
- Requirement 2. Sensitivity to metrics' criticality. In many cases, it is possible to rank the metrics based on their criticality for a given information system and task. The algorithm should consider the criticalities of the security, safety, privacy, resilience, and reliability metrics being integrated if such information is available.
- Requirement 3. Non-reduction in the maximum risk score of the metrics being integrated. In the case when metrics have equal criticality, the algorithm should preserve the maximum value among integrating metrics, avoiding reducing integral score when one of the metrics has a high or small risk score relative to other ones.
- Requirement 4. Easy to use and configure. The use and setting parameters of the algorithm for integrating a set of trustworthiness metrics should be easy and transparent to the end-user.

Requirements 1, 2, and 4 are quite standard, while Requirement 3 directly relates to the motivation for the algorithm design. The goal of the research is to elaborate an algorithm that takes as an input a set of risk-aware metrics of different types and origins and outputs an integral risk score that could be used by an end-user to make a reasonable decision about an object's trustworthiness level. The authors noticed that, in some cases, when applying a weight averaging algorithm for aggregating risk-aware metrics with a high or small value, the overall risk score is reduced, thus leading to the deceptive conclusion that integral risks are lower when they are. This could be especially confusing in the case when the consumer of the metric is the end-user who has no access to all components of the integral risk score or has no or little knowledge of how to explain it and therefore requires only one clear and transparent metric.

To make Requirement 3 valid and meaningful, it is necessary to define requirements to the input metrics. The input metrics are the risk score metrics, where the higher value corresponds to the higher risk level. Examples of such metrics could be a privacy risk score that reflects the risk score relating to privacy issues of the analyzed object, i.e., information system, its sub-component or device, security risk score that reflects risks associated with confidentiality, integrity, and availability issues of the object, reliability risk score that reflects risk score associated with the ability of the object "to operate under designated operating conditions for a designated time or number of cycles" [26].

The underlying idea of the algorithm proposed is as follows. The metric with the highest risk score or with the highest criticality, if such data are available, serves as a basis, and the values of other metrics, including their criticality, define an additive coefficient that increases the basis value. This coefficient has to consider its weights, current values, and possible maximum values. The authors suggest applying a nonlinear logarithm function to calculate it. It allows one to avoid the fast growth of integral metric value, as with higher values of argument the logarithm function slows down the growth of output value.

Let $METRIC\_VALS$ be a list of n metrics' values; it is required that the range of all metrics' values is to be normalized to the range [0, 10]. Let MAX_VAL constant be a possible maximum value of the metric, i.e., MAX_VAL equals 10. Let $METRIC\_WEIGHTS$ be a list of weights for the given list of metrics; the weights reflect the criticality of the given metrics, and their sum equals 1. The calculation of the integral trustworthiness risk score is presented in Algorithm 1.

Algorithm 1 Integral trustworthiness risk score calculation.

Input: $METRIC\_VALS$, $METRIC\_WEIGHTS$, MAX_VAL
Output: *integral_score*

if $METRIC\_VALS$ is empty **or** all values are not defined (or null) **then**
    return return not defined (or null)
end if
if all elements of $METRIC\_WEIGHTS$ are equal to each other **then**
    set *base_score* as a maximum element of $METRIC\_VALS$
else
    set *base_score* as an element from $METRIC\_VALS$ with highest weight from $METRIC\_WEIGHTS$
end if
exclude the metric chosen as *base_score* from $METRIC\_VALS$, and exclude corresponding weight from the $METRIC\_WEIGHTS$
calculate logarithm base *log_base* as follows:

$$log\_base = 1 + \sum_{i=0}^{n-2} MAX\_VAL * METRIC\_WEIGHTS[i]$$

calculate *integral_score* as follows:

$$integral\_score = base\_score + \log_{log\_base}(1 + \sum_{i=0}^{n-2} METRIC\_VALS[i] * METRIC\_WEIGHTS[i])$$

if *integral_score* > 10 **then**
    set *integral_score* as 10
end if
return *integral_score*

The algorithm outputs the integral score *integral_score* in the range $[0, 10]$. It could be shown that the maximum value for the additional additive coefficient is 1 and is reached when all metrics have a maximum score, excluding the one selected as a basis. Thus, in some cases, when all risk scores take high scores, i.e., equal or close to 10, the integral risk score exceeds the upper bound of the possible range, and it is necessary to apply truncation operation. However, the maximum truncated portion equals 1, and the truncated integral score still takes the highest value; thus, its semantic meaning is not corrupted. It should be also noted that a similar approach is used in the Common Vulnerability Scoring System [3] that is used worldwide to assess the severity of the software vulnerabilities.

The following two small examples illustrate the calculation procedure of the integral trustworthiness risk score.

For the sake of simplicity and without loss of generality, let us consider a set of three metrics for trustworthiness risk score calculation—security risk score based on the assessment of confidentiality, integrity, and availability state of the system (further referred as CIA score), privacy, and reliability risk scores. Privacy is not equal to the CIA-based security, and having a security system does not guarantee low risks in privacy, as they are associated with transparency of data processing that assumes a clear understanding of what data and what purposes of their processing are. Let their values be 4.6, 3.0, and 5.5, correspondingly. Let all metrics have equal significance, and therefore their weights are equal to each other (0.33). The maximum score is the reliability score, and it serves as the basis of the integral score. Then the integral trustworthiness risk score is calculated as follows: $integral\_score = 5.5 + log(1 + (0.33 * 3.0 + 0.33 * 4.6), 1 + 0.33 * 10 * 2) = 6.1$.

Let us consider the similar example; however, the metrics are assigned different criticality level resulting in the following weights: weight of CIA score is 0.6, weight of privacy score is 0.1, weight of reliability score is 0.3. Then, the base score is defined

by a metric with the maximum weight, and it is a CIA score. Then, the final integral trustworthiness score is calculated as follows: $integral\_score = 4.6 + log(1 + (0.1 * 3.0 + 0.3 * 5.5), 1 + 0.1 * 10 + 0.3 * 10) = 5.3$.

4. Sensitivity Analysis of the Proposed Algorithm

In the proposed algorithm, the impact of the changes in metrics' values that are used in calculation of the integral trustworthiness score depends on their criticality. Let $\mathbf{M} = \{m_0, m_1, \cdots, m_n\}$ be a set of n metrics with corresponding weights $\mathbf{W} = \{w_0, w_1, \cdots, w_n\}$. Let m_{max} be a maximum value that m_i can take.

The basis of the integral risk score is defined by the metric with the largest value or with the largest weight, if such information is available. Let m_0 be a metric with the highest value or criticality without loss of generality. Then, the formula for calculating the trustworthiness integral score is as follows:

$$integral\_score = m_0 + \log_{(1+\sum_{i=1}^{n-1} m_{max} * w_i)}(1 + \sum_{i=1}^{n-1} m_i * w_i). \tag{1}$$

Let the value of metric m_0 changes for Δm, and new value is defined as $m_0' = m_0 + \Delta m$, then a novel value for integral score $integral\_score'$ is calculated as follows:

$$\begin{aligned} integral\_score' &= m_0' + \log_{(1+\sum_{i=1}^{n-1} m_{max} * w_i)}(1 + \sum_{i=1}^{n-1} m_i * w_i) \\ &= m_0 + \Delta m + \log_{(1+\sum_{i=1}^{n-1} m_{max} * w_i)}(1 + \sum_{i=1}^{n-1} m_i * w_i). \end{aligned} \tag{2}$$

From Formulas (1) and (2), it follows that

$$\Delta integral\_score = integral\_score' - integral\_score = \Delta m.$$

Let us consider the case when the weight of m_0 is not the highest one, i.e., $w_0 \leq w_i$ for $i = 1 \ldots n$. Let m_1 be a metric with the highest value or criticality without loss of generality.

$$integral\_score = m_1 + \log_{(1+\sum_{i=0, i\neq 1}^{n-1} m_{max} * w_i)}(1 + m_0 * w_0 + \sum_{i=2}^{n-1} m_i * w_i). \tag{3}$$

Let a new value of m_0 be defined as $m_0' = m_0 + \Delta m$, where Δm is a change in its value. Then, a novel value for integral score $integral\_score'$ is calculated as follows:

$$\begin{aligned} integral\_score' &= m_1 + \log_{(1+\sum_{i=0, i\neq 1}^{n-1} m_{max} * w_i)}(1 + m_0' * w_0 + \sum_{i=2}^{n-1} m_i * w_i) \\ &= m_1 + \log_{(1+\sum_{i=0, i\neq 1}^{n-1} m_{max} * w_i)}(1 + (m_0 + \Delta m) * w_0 + \sum_{i=2}^{n-1} m_i * w_i). \end{aligned} \tag{4}$$

From Formulas (3) and (4), it follows that

$$\begin{aligned} &\Delta integral\_score = integral\_score' - integral\_score \\ &= \log_{(1+\sum_{i=0, i\neq 1}^{n-1} m_{max} * w_i)}(1 + (m_0 + \Delta m) * w_0 + \sum_{i=2}^{n-1} m_i * w_i) \\ &\quad - \log_{(1+\sum_{i=0, i\neq 1}^{n-1} m_{max} * w_i)}(1 + m_0 * w_0 + \sum_{i=2}^{n-1} m_i * w_i) \\ &= \log_{(1+\sum_{i=0, i\neq 1}^{n-1} m_{max} * w_i)}\left(1 + \frac{\Delta m * w_0}{1 + \sum_{i=0, i\neq 1}^{n-1} m_i * w_i}\right). \end{aligned} \tag{5}$$

Thus, it is possible to conclude that, if the value of the metric with the highest criticality changes, then the integral metric changes by the same value. The impact of the changes of the rest metrics is not so significant as it is defined by a logarithm from the criticality of the metric, i.e., its weight, and change in its value. The more a metric changes, the more significant its impact. However, it should be noted that, for the case when all metrics are equally significant, i.e., their weights are equal to each other, the impact of changes in metrics also depends on its amount. If a given metric becomes a metric with the highest value after its value has changed, then it starts defining a base for calculating an integral security metric.

It is also easy to show that, in the algorithms based on weighted sum, the impact of change is always defined by the product of the metric's weight and by the difference between its current and the previous value.

5. Experiments and Discussion

To analyze the difference between the proposed algorithm and the weighted sum properly, the authors implemented a set of experiments.

Experiment 1. We considered the case when three metrics are used to calculate integral trustworthiness risk score—CIA risk score, privacy risk score, and reliability risk score. Let all these metrics be equally meaningful, that is why corresponding weights were set equal to each other (0.33). Then, we evenly changed the values of the reliability score from 0.0 to 10.0, while the value of the CIA score was fixed at 1.0, 5.0, and 10.0, alternately, and the privacy score was fixed to 5.0. Such experimental settings allowed the authors to observe how the function behaves on limit values of the input metrics, to demonstrate its difference from the weight averaging function, and to use visualization to show the behavior of the function more clearly.

Figure 1 shows the difference in the values of the integral trustworthiness risk score (integral risk score) when it is calculated using the weighted sum (weight integral score) and the proposed nonlinear weighted algorithm (weight nonlinear integral score). When the weighted sum was used, the weight integral score changed linearly in ranges whose length is equal to 3.3: [2.0, 5.3], [3.3, 6,6], and [5.0, 8.3].

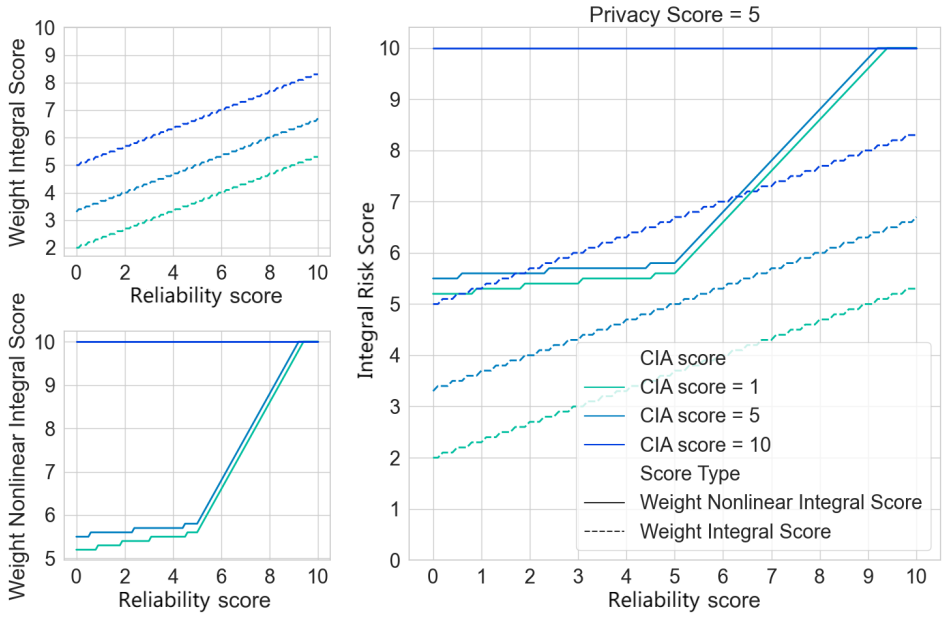

Figure 1. The character of the integral risk scores calculated using weighted sum function (weight integral score) and proposed nonlinear weight function (weight nonlinear integral score) for three metrics being integrated: privacy score set to 5, CIA score set to 1, 5, and 10, and reliability score varying from 0 to 10.

A weight nonlinear integral score depends on the highest value of one of the three metrics used. That is why its initial value is 5.3 or 5.6 for CIA score set to 1.0 or 5.0. Then, it slightly grows when the reliability score is less than 5.0 and increases quickly when the reliability score is greater than 5.0 and grows. The weight nonlinear integral score equals 10.0 in the case when CIA score is set to 10, even when CIA is fixed to 1.0. The linear weighted algorithm reaches the highest integral score of 10.0 only if all metrics are set to maximum.

Experiment 2. In the previous experiment, we used the same weights for CIA score, privacy score, and reliability score. In this set of experiments, we evaluated how the changes in weights affect the integral score and also compared the results with the weighted sum function. Privacy score was fixed to 5.0 with a weight of 0.2 and the CIA score was fixed to 5.0, but its weight was set to 0.2 in the first case, and 0.6 in the second case. The reliability score varied from 0.0 to 10.0, and its weight was set to 0.6 in the first case is 0.6 and to 0.2 in the second case. Thus, the first case reflects how the integral score changes with the growth of the most important metric with the greatest weight. The second case shows a change in the integral score when the most significant metric is fixed.

Figure 2 shows the integral scores for the weighted sum algorithm (weight integral score) and the weighted nonlinear algorithm (weight nonlinear integral score). We can conclude that, with the growth of the most significant metric with the highest weight, the integral score grows faster and reaches the maximum value earlier if the weighted nonlinear algorithm is used. An increase in an insignificant metric for both algorithms is comparable.

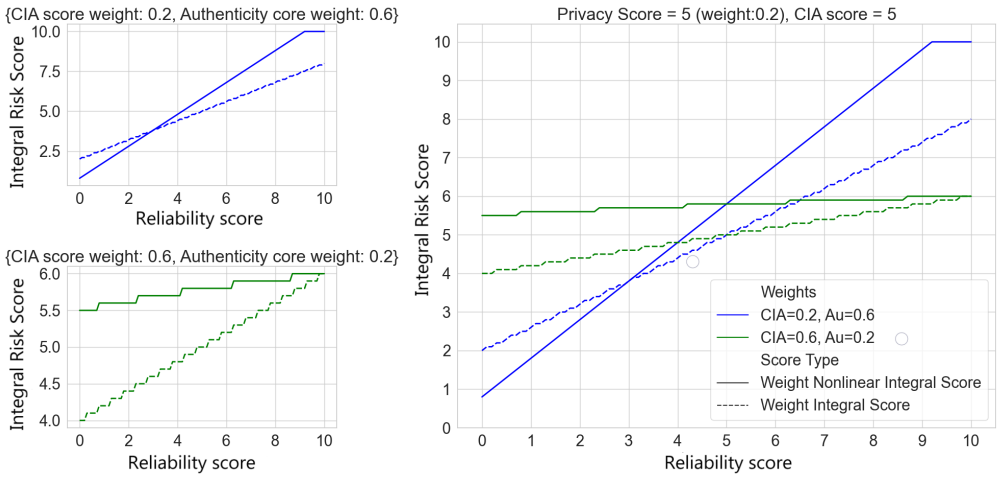

Figure 2. Impact of metric weights on the integral risk scores calculated using weighted sum function (weight integral score) and proposed nonlinear weight function (weight nonlinear integral score).

Experiment 3. In the third series of experiments, we tested the dependence of the proposed algorithm on a different number of security metrics.

Figure 3 shows the difference in the values of the integral score when it is calculated using the weighted sum and the proposed algorithm for a different number of metrics used. The first row of plots in Figure 3 corresponds to the calculation of the integral score on two metrics—CIA and reliability scores—while both change their value from 0.0. to 10.0 and have weights equal to 0.5. The second row of plots in Figure 3 shows the calculation of the integral score for three metrics, adding a fixed privacy score with a value of 5.0 to the previous case. The weight of each metric is set to 0.33. Finally, the third row of plots in Figure 3 contains the integral score for four metrics, where a safety score is added with a fixed value of 5.0, and each metric weight is 0.25. We can see that the character of the integral weighted score and the weight nonlinear integral score is different for different cases of metrics.

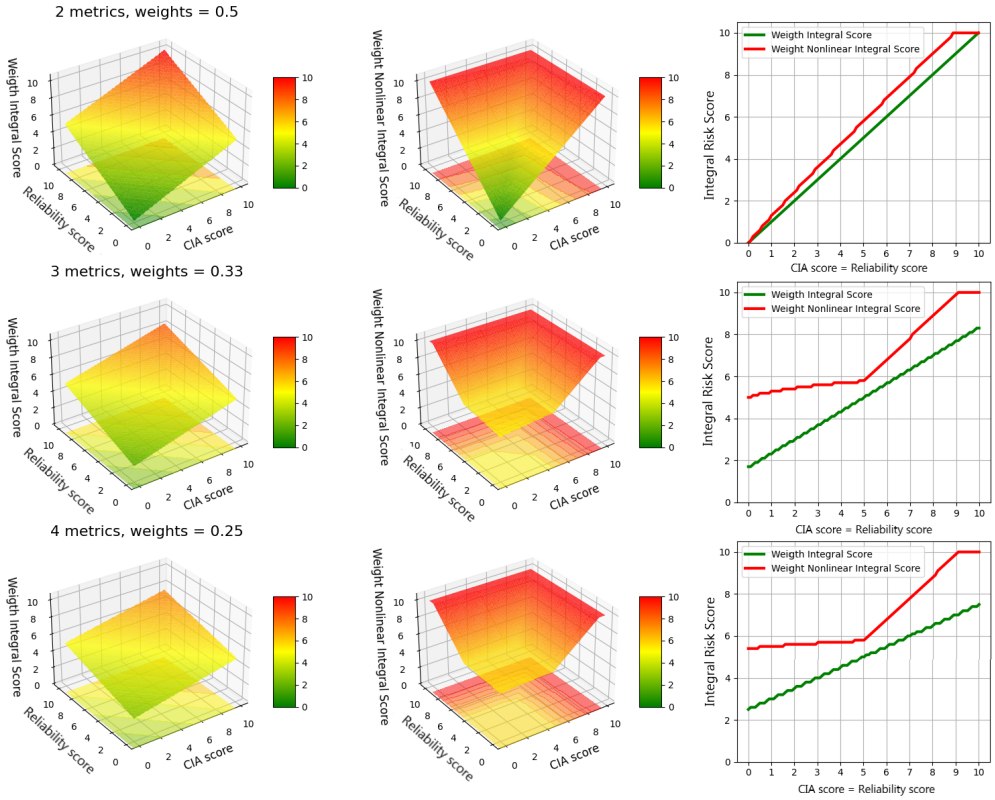

Figure 3. Integral risk score values using a weighting algorithm and using the proposed nonlinear weighting algorithm. The rows show calculations for a different number of metrics.

It is seen that the range of values of the weight integral score produced by the weighted sum algorithm decreases when the number of metrics with similar values increases. Its range lies in the neighborhood of these values and it changes linearly. Thus, the algorithm based on weighted sum reduces the values of the integral score when one metric has either a high or small score relative to other metrics, because for the case when all metrics are equally important it acts as an averaging filter. The proposed weighted nonlinear algorithm does not reduce the highest value of the metric, as it is selected as a base for the integral score, and this base is increased proportionally to the values of the rest metrics.

Figure 3 shows that integral score grows slowly when the CIA and reliability scores are either small or comparable with privacy score or safety score, but when these two metrics become greater than other metrics (more than 6), the integral score starts growing faster reaching the highest score. So, it could be concluded that the proposed algorithm produces cumulative scores.

We also compared the proposed approach to the existing ones, and Table 1 summarizes the results of this analysis. The serious drawback of table-based approaches is a lack of scalability. Setting the values of the integral metric in tabular form is easy and transparent when the number of metrics that are used to define it are limited to 3, and this process becomes very complicated when their quantity exceeds 3.

The min–max approach does not lead to reducing the integral score when one of the metrics has a high or small score relative to other ones. However, it is not sensitive to metrics criticality and is not easy to use and configure. Besides, while the min–max approach is scalable, it requires additional tuning of the integral metric while adding new components.

The weighted sum approach is highly scalable; it considers the ranks of metrics, and its output is easy to understand and explain. However, in the cases when all input metrics are considered equally meaningful, i.e., their criticalities are equal, it simply averages their values, outputting the value that is less than the maximum value of integrated metrics. Such

reduction in integral score could be critical in trustworthiness assessment and management procedures when the output is in border values for decision making.

Table 1. Comparison of existing approaches to the integral metric calculation.

	Approach	Req. 1	Req. 2	Req. 3	Req. 4
1	Table-based approach [1]	−	+	+	+ / −
2	Min–max based approach [2]	+ / −	−	+	−
3	Weighted sum approach [3]	+	+	−	+
4	Our approach	+	+	+	+

6. Conclusions

Analysis of the relevant research showed that calculating the trustworthiness metric is one of the cyber security challenges nowadays. The paper introduced a novel algorithm, developed by the authors, for integral trustworthiness risk score calculation that is scalable to any number of metrics, considers their criticality, and does not perform averaging in a case when all metrics are of equal importance.

The resulting metric can be further transformed to characterize trustworthiness level to support a clearer understanding of the system or device trust level. Though this transformation is not discussed in the article, the calculated integral trustworthiness risk score calculated for the device on the basis of its privacy, reliability, resilience, safety, and CIA risk scores can help users to compare different devices in terms of the trust. The same integral score for the system can be used by organizations to compare the system trustworthiness risk level at different time moments.

In order to produce the meaningful integral trustworthiness risk score, the authors also identified the requirements for the input metrics. The input metrics are to be risk-aware metrics, where higher value corresponds to the higher level of the corresponding risk. The range of values has to be normalized to the range [0, 10]. There is no strict requirement to the procedures that are used to calculate such metrics; they could be defined either on a table-based basis or probability-based basis. However, to be able to use an output integral trustworthiness risk score to compare the trust level of the devices, the procedures used to calculate its input components should be consistent and similar for each assessed device.

The algorithm operation was demonstrated in the examples. The sensitivity analysis showed that the value of the produced integral metric highly depends on the value of the metric with the highest criticality, while the impact of the changes of the rest metrics is not so significant. It was also approved by the experimental analysis. Thus, the proposed weighted nonlinear algorithm does not reduce the highest value of the metric. Meanwhile, in the algorithms based on weighted sum, the impact of change is always defined by the product of the metric's weight and by the difference between its current and the previous value. Thus, the algorithm based on weighted sum reduces the values of the integral score when one metric has either a high or small score relative to other metrics, because for the case when all metrics are equally important it acts as an averaging filter. Such reduction in integral score could be critical in trustworthiness assessment and management procedures when the output is in border values ranges for decision making.

Author Contributions: Conceptualization, E.N., E.D., and I.K.; methodology, E.N., E.D., and I.K.; software, E.N., and D.G.; validation, E.N., D.G., and E.D.; formal analysis, E.N., D.G., E.D., and I.K.; investigation, E.N., E.D., and D.G.; writing—original draft preparation, E.N., D.G., and E.D.; writing—review and editing, E.N., E.D., and I.K.; visualization, D.G., and E.N.; supervision, I.K.; funding acquisition, I.K. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the grant of RSF #21-71-20078 in SPC RAS.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Peltier, T.R. *Information Security Risk Analysis*, 3rd ed.; CRC Press: Boca Raton, FL, USA, 2005; 456p.
2. Khouzani, M.; Liu, Z.; Malacaria, P. Scalable min-max multi-objective cyber-security optimisation over probabilistic attack graphs. *Eur. J. Oper. Res.* **2019**, *278*, 894–903. [CrossRef]
3. Common Vulnerability Scoring System v3.1: Specification Document. Available online: https://www.first.org/cvss/specification-document (accessed on 15 November 2021).
4. Huo, L.; Persson, H.J.; Lindberg, E. Early detection of forest stress from European spruce bark beetle attack, and a new vegetation index: Normalized distance red & SWIR (NDRS). *Remote Sens. Environ.* **2021**, *255*, 112240. [CrossRef]
5. Tao, H.; Wu, H.; Chen, Y. An Approach of Trustworthy Measurement Allocation Based on Sub-Attributes of Software. *Mathematics* **2019**, *7*, 237. [CrossRef]
6. Tao, H.; Wu, H.; Chen, Y. Tao, H.; Wu, H.; Chen, Y.; Tao, H.; Chen, Y.; Wu, H. A Reallocation Approach for Software Trustworthiness Based on Trustworthy Attributes. *Mathematics* **2020**, *8*, 14. [CrossRef]
7. Payne, S.C. A Guide to Security Metrics. SANS Institute Information Security Reading Room. 2006. Available online: https://www.sans.org/white-papers/55/ (accessed on 15 November 2021).
8. Bodeau, D.J.; Graubart, R.D.; McQuaid, R.M.; Woodill, J. *Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods*; Technical Report; The MITRE Corporation: Bedford, MA, USA, 2018.
9. Chew, E.; Swanson, M.M.; Stine, K.M.; Bartol, N.; Brown, A.; Robinson, W. *Performance Measurement Guide for Information Security*; NIST Special Publication 800-55 Revision 1; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2008. [CrossRef]
10. Bakshi, A.; Ahmad, K.; Kumar, N. Security Metrics: Needs and Myths. *Int. Trans. Math. Sci. Comput.* **2011**, *4*, 31–40.
11. *ISO/IEC 27005*; Information Technology—Security Techniques—Information Security Risk Management. International Organization for Standardization: Vernier, Switzerland; Geneva, Switzerland, 2018; p. 56.
12. Man, D.; Yang, W.; Yang, Y.; Wang, W.; Zhang, L. A quantitative evaluation model for network security. In Proceedings of the 2007 International Conference on Computational Intelligence and Security (CIS 2007), Harbin, China, 15–19 December 2007; pp. 773–777. [CrossRef]
13. Doynikova, E.; Kotenko, I. CVSS-based Probabilistic Risk Assessment for Cyber Situational Awareness and Countermeasure Selection. In Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP 2017), St. Petersburg, Russia, 6–8 March 2017; pp. 346–353. [CrossRef]
14. Kotenko, I.; Doynikova, E. Dynamical calculation of security metrics for countermeasure selection in computer networks. In Proceedings of the 24th Euromicro International Conference on Parallel, Distributed and Network-Based Processing (PDP 2016), Heraklion, Greece, 17–19 February 2016; pp. 558–565. [CrossRef]
15. Granadillo, G.G.; Débar, H.; Jacob, G.; Gaber, C.; Achemlal, M. Individual countermeasure selection based on the return on response investment index. In Proceedings of the International Conference on Mathematical Methods, Models, and Architectures for Computer Network Security, St. Petersburg, Russia, 17–19 October 2012; pp. 156–170. [CrossRef]
16. Gordon, L.A.; Loeb, M.P. The economics of information security investment. *ACM Trans. Inf. Syst. Secur.* **2002**, *5*, 438–457. [CrossRef]
17. RiskWatch. Available online: http://www.riskwatch.com (accessed on 11 November 2021).
18. Common Weakness Scoring System (CWSS). Available online: https://cwe.mitre.org/cwss/cwss_v1.0.1.html (accessed on 15 November 2021).
19. Tilei, G.; Tong, L.; Ming, Y.; Rong, J. Research on a Trustworthiness Measurement Method of Cloud Service Construction Processes Based on Information Entropy. *Entropy* **2019**, *21*, 462. [CrossRef] [PubMed]
20. Mohammadi, N.G. *Trustworthy Cyber-Physical Systems: A Systematic Framework towards Design and Evaluation of Trust and Trustworthiness*, 1st ed.; Springer Vieweg: Wiesbaden, Germany, 2018; 320p. [CrossRef]
21. Cho, J.H.; Xu, S.; Hurley, P.M.; Mackay, M.; Benjamin, T.; Beaumont, M. STRAM: Measuring the Trustworthiness of Computer-Based Systems. *ACM Comput. Surv.* **2019**, *51*, 47. [CrossRef]
22. Savage, S.L. *The Flaw of Averages: Why We Underestimate Risk in the Face of Uncertainty*, 3rd ed.; Wiley: Hoboken, NJ, USA, 2009.
23. Zhang, P.; Durresi, A.; Barolli, L. Survey of Trust Management on Various Networks. In Proceedings of the 2011 International Conference on Complex, Intelligent, and Software Intensive Systems, Seoul, Korea, 30 June–2 July 2011; pp. 219–226. [CrossRef]
24. Alhadad, N.; Lamarre, P.; Busnel, Y.; Serrano-Alvarado, P.; Biazzini, M.; Sibertin-Blanc, C. SocioPath: Bridging the Gap between Digital and Social Worlds. In *Database and Expert Systems Applications*; Liddle, S.W., Schewe, K.D., Tjoa, A.M., Zhou, X., Eds.; Springer: Berlin/Heidelberg, Germany, 2012; pp. 497–505.
25. Hiltunen, J.; Kuusijärvi, J. Trust Metrics Based on a Trusted Network Element. In Proceedings of the 2015 IEEE Trustcom/BigDataSE/ISPA, Helsinki, Finland, 20–22 August 2015; Volume 1, pp. 660–667. [CrossRef]
26. Leimeister, M.; Kolios, A. A review of reliability-based methods for risk analysis and their application in the offshore wind industry. *Renew. Sustain. Energy Rev.* **2018**, *91*, 1065–1076. [CrossRef]