A Quantitative CVSS-Based Cyber Security Risk Assessment Methodology For IT Systems

M. Ugur Aksu[1], M. Hadi Dilek[1], E. İslam Tatlı[1], Kemal Bicakci[2], H. İbrahim Dirik[1], M. Umut Demirezen[1], Tayfun Aykır[1]
[1]Cyber Security And Big Data Directorate
[1]STM Defense Technologies Engineering and Trade Inc. Ankara, Turkey
[1]{mugur.aksu, mhdilek, emin.tatli, hidirik, udemirezen, taykir}@stm.com.tr
[2]Computer Engineering Department
[2]TOBB University of Economics and Technology Ankara, Turkey
[2]bicakci@etu.edu.tr

***Abstract*—IT system risk assessments are indispensable due to increasing cyber threats within our ever-growing IT systems. Moreover, laws and regulations urge organizations to conduct risk assessments regularly. Even though there exist several risk management frameworks and methodologies, they are in general high level, not defining the risk metrics, risk metrics values and the detailed risk assessment formulas for different risk views. To address this need, we define a novel risk assessment methodology specific to IT systems. Our model is quantitative, both asset and vulnerability centric and defines low and high level risk metrics. High level risk metrics are defined in two general categories; base and attack graph-based. In our paper, we provide a detailed explanation of formulations in each category and make our implemented software publicly available for those who are interested in applying the proposed methodology to their IT systems.**

***Index Terms*—attack graphs, cyber security risks, risk assessment, risk metrics, vulnerability management**

I. Introduction

Risk Assessment in IT systems is the process of identifying, estimating and prioritizing information security risks. It is a critical component of the overall risk management strategy [1]. By conducting risk assessments, organizations know how vulnerable their IT infrastructure and assets are, and plan the required mitigation methods accordingly [2].

As the number of and reliance on IT systems, applications, and data assets increase, risk assessment and mitigations gain more importance [2] [3]. Increasing cyber threats urge organizations to measure the security level of their systems continuously and conduct risk assessments to spot the weaknesses on their IT systems and minimize exposures to likely threats by remediating the risks in a prioritized manner [4]. In addition, laws, mandates, regulations and standards such as Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Federal Information Security Management Act (FISMA), Sarbanes-Oxley Act (SOX) and ISO 27001 [5] require organizations to conduct periodic risk and vulnerability assessments and implement defined security controls.

Risk management frameworks and methodologies such as NIST standards [1] [6], Facilitated Risk Analysis Process (FRAP), Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) and ISO Information Security Risk Management Standard (ISO/IEC 27005) are commonly used industry standards. Among them, NIST SP 800-30/37, ISO/IEC 27005 and OCTAVE are IT-specific cyber security risk models. Such high level frameworks or standards define structured approaches or guidance on how to assess risks while showing serious deficiencies as a metrics framework. With insufficient attention to measurement, these frameworks mainly focus on auditing with taxonomies well-defined for the information security domain but they miss details for the specific risk metrics and automatic methods for calculating the risks [7].

In our study, we define a metrics-focused risk assessment methodology for IT systems to overcome such drawbacks of the high level risk frameworks and methodologies. The risks of an IT system are represented quantitatively in two general categories; base and attack graph-based. The analysis approach is both asset and vulnerability-centric. Vulnerabilities in a system are defined with Common Vulnerabilities and Exposures (CVE) IDs.

For risk assessment, we make use of Common Vulnerability Scoring System (CVSS) [8]. Due to its focus on scoring single CVEs, CVSS uses a formulation and normalization approach different from our methodology. For this reason, CVSS scores are not used directly. We derive risk formulations from the general risk formulation *(Risk = Probability * Impact)* and generate different risk views. Preserving the semantics whenever possible, we utilize CVSS metrics and assign new numeric values to them if needed. Moreover, we propose new low level metrics and define high level risk metrics on top of low level metrics.

The rest of the paper is organized as follows. Section 2 reviews background information. Section 3 defines our risk assessment methodology and explains low level risk metrics. Section 4 presents our suggested high level risk metrics. Section 5 reviews related work and Section 6 concludes the paper with future work.

II. Background

To assess the risk of a system, first, the metrics - standards of measurements - needs to be defined. However, in IT domain, security metrics are relatively immature and far from being

978-1-5386-1585-0/17/$31.00 ©2017 IEEE

comprehensive compared to other fields such as operations management [9]. Thus there is definitely a need to define new metrics specific for information systems. To be useful, though, a good metric should be repeatable (consistently measured), be cheap to gather, be context specific and have a unit of measure [7].

After defining the metrics as units of measures for risk assessment, another milestone is the description and identification of vulnerabilities. For this purpose, as unique identifiers, CVEs are commonly used for cyber security vulnerabilities. For communicating the characteristics, impacts and risks of almost all of these CVEs, using the open framework named CVSS is a common practice [8]. Sharing the risk scores and underlying metrics of known vulnerabilities through public vulnerability databases, CVSS provides a foundation for developing and measuring network security metrics [10]. Since, currently CVE database for the CVSS 3.0 [11] is not as complete as CVSS 2.0, in our work we use CVSS 2.0 metrics. However, our work can be easily adapted to the version 3.0.

For single vulnerabilities, CVSS provides a calculation method that comprises of ordinal type metrics in three categories, (i.e. base, temporal and environmental) and gives risk scores for each category. Base metrics are the innate characteristics of the vulnerabilities while the temporal metrics are those that change over time due to events external to the vulnerabilities. Environmental metrics on the other hand are custom metrics relevant and unique to a particular users environment. CVSS 2.0 metrics that are utilized in this work are depicted at Table I. For further information about CVSS 2.0 metrics, we refer to [8].

TABLE I
CVSS 2.0 METRICS UTILIZED IN THIS WORK

Base	**Temporal**	**Environmental**
Access Vector	Exploitability	Confidentiality Req.
Access Complexity	Remediation Level	Integrity Req.
Authentication	Report Confidence	Availability Req.
Confidentiality Impact		
Integrity Impact		
Availability Impact		

III. OUR METHODOLOGY FOR RISK ASSESSMENT

We define our risk assessment methodology in four steps [1]:

- An assessment approach (quantitative, qualitative),
- An analysis approach (threat-oriented, asset/impact-oriented, or vulnerability oriented),
- An explicit risk model,
- A risk assessment process.

A. Risk Assessment Approach

Risk assessments can be held *quantitatively* or *qualitatively*. Quantitative risk assessments require monetary or numerical values for risk factors whereas qualitative methods employ non-numeric priority or criticality values. We employ a quantitative approach in our model due to three reasons. First, the underlying metrics of the CVSS has numerical values assigned to them since the CVSS is a quantitative approach. Second, in quantitative approach, the evaluation and the results are based on objective criteria and thus more suitable for an IT system risk assessment. Lastly, quantitative approach is more suited for measuring the security level of an IT system in terms of the three common security pillars (confidentiality, integrity and availability) [3].

B. Analysis Approach

Regarding the analysis approach, assessments can be held in a *threat/attacker oriented* , *asset/impact oriented* or *vulnerability/architecture oriented* way. Each analysis approach takes into consideration the same risk factors. What differs in each approach is the order of the factors taken into account, thus the importance given to the different factors in each approach changes, which results in a bias introduced to the assessment results [1].

Vulnerability/architecture centric models focus on system design or vulnerabilities and attacks against each component/vulnerability. Asset/impact centric models identify asset values and impacts on the assets by taking the motivation and capability of the threat sources into account. Threat/attacker centric models put more emphasis on the properties of the attack sources through identifying an attacker and focusing on the attackers goals and techniques to assess the risk.

Among the three types of risk analysis models, our work fits to the asset and vulnerability centric models, for two reasons. First, threat centric model requires threat intelligence in order to identify attackers specifically, which is beyond the scope of our work. Second, by defining a number of high level metrics, we quantify the risks of both individual assets and the vulnerabilities at the assets, hence satisfying the considerations of the asset and vulnerability centric models.

C. Risk Assessment Model

In this section, the semantics of the risk assessment model is defined in general terms. A detailed explanation together with calculation formulas for each of the components are given in the following sections. We define two different risk assessment models; one for base risk assessment and another for attack graph-based risk assessment, as depicted in Fig. 1 and 2.

Fig. 1. Base Risk Assessment Model

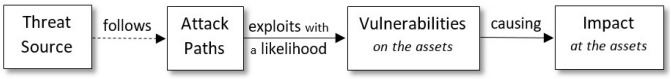

Fig. 2. Attack Graph-Based Risk Assessment Model

Base risk assessment model comprises of four components; *assets, vulnerabilities, likelihoods* and *impacts* (attackers are unknown sources with no known parameters. For this reason, threat source in the Fig. 1 is depicted with dashed box).

Attach-graph-based risk assessment model comprises of six components, adding two additional components to the first model, which are the *threat sources* and *attack paths*. The attack graph-based model differs from the base model mainly because the probability is not calculated using only the CVSS metrics of the CVEs, but also taking both the capabilities of the threat sources and the attack paths of the exploitations. Thus, attack graph-based risk assessment enables us to quantify risks for single or multiple attack paths and/or attack sources.

The basic tangible elements of risk in an IT system can be enumerated as assets, vulnerabilities, and threats. In our model, an asset is any computer or network equipment, physical or virtual, on which software related vulnerabilities might exist. We also define the term product as software which might have any vulnerabilities on them. Assets might have one or more products on them.

Asset valuations are made on a scale of low, medium, or high according to CIA requirements due to two reasons. First, information security risks arise from the loss of confidentiality, integrity, or availability of information or information systems [1]. Second, FIPS 199 provides information classification as low, medium, or high security based upon the CIA criteria of the assets [12].

Vulnerabilities in a system are those defined in the NVD vulnerability database with their specific CVE IDs. The list of relevant vulnerabilities in a given system could be generated by scanning the system with vulnerability detection tools such as OPENVAS, Nessus etc. Furthermore, for the attack graph-based model, vulnerabilities in a system can be filtered out to identify which of them are not applicable and cannot be exploited, taking into account the protection of tools such as IDS/IPS residing on the attack paths. Thus, vulnerabilities labeled as protected are disregarded for risk calculations.

Vulnerabilities are exploited with a probability that is determined by the low level metrics derived from the underlying metrics of the vulnerabilities, threat sources and attack paths. In the base model, probabilities corresponding to exploiting CVEs are assumed to be independent thus probability calculation of a single CVE is not affected when there are multiple CVE exploits on an asset. Attack graph-based model, however, considers the probabilities of previous CVEs on the attack path for calculating the probability of CVE exploitation.

Impacts are defined as confidentiality, integrity and availability (CIA) losses at the assets if CVEs are exploited successfully on them. Impacts are computed according to the CIA requirements of the assets and the CIA impacts of the vulnerabilities residing on them.

Threat sources in the model are defined as attackers which could be either hackers attacking from the Internet or malicious users attacking from a specific location inside the network that is under assessment. In the attack graph-based model, threat sources are denoted by two parameters, capability and motivation. Capability of a threat source is the measure of how able a threat source in exploiting the known vulnerabilities. Motivation, on the other hand, shows the extent to which an attacker is willing and resolute in capturing a target via exploitations of the vulnerabilities.

Attack paths or attack graphs show how multiple vulnerabilities may be combined for an attack. In our approach, attack graphs are a number of vulnerabilities on the assets with directed connections between each of them, depicting the cycle free exploitation orders. Vulnerability exploitations on attack graphs are showed as transitions between states [13]. Generating the attack graphs is out of scope in our work (attack graphs can be generated as described by earlier studies e.g., [13]) Fig. 3 illustrates an example attack graph model.

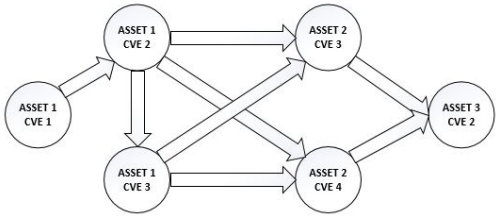

Fig. 3. An Example Attack Graph Model

D. Risk Assessment Process

Conducting risk assessment and defining the related metrics in this context can be explained in the following order: (1) Identify threat sources, (2) Identify vulnerabilities, (3) Determine likelihood of occurrence, (4) Determine magnitude of impact, and (5) Determine risk.

In our model, threat sources are defined on the attack graphs with their location, capability and motivation parameters. Vulnerabilities can be found out on the assets with vulnerability scanning tools, as stated previously. For probabilities of occurrences, it can be determined in two ways depending on the risk assessment model.

For the *base risk assessment* , we do not take the properties of threat sources into account for probability calculation. We assume that a threat source exploits a CVE with a probability calculated from the underlying CVSS metrics of the CVE explained below. Probability calculation formula is given in (1) and the employed metrics together with assigned numeric values are described at Table II.

The numerical values for the risk metrics, depicted in the following tables, have been assigned based on available evidence, experience and expert judgement (utilizing from the CVSS 2.0 [8] numerical metric values) and can be modified according to possibly different judgements and experience.

$$P = AV * AC * Au * E * RC \tag{1}$$

For the *attack graph-based risk assessment*, the semantics of Access Vector (AV) metric is already incorporated into the attack graph which is used as an input to our risk assessment model. Therefore, AV metric is not directly used in the

TABLE II
BASE RISK: LOW LEVEL METRICS FOR PROBABILITY CALCULATION

Metric	Abb.	CVSS	Metric Val.	Abb.	Num. Val.
Access Vector	AV	Base	Local Adjacent Network	L A N	0,4 0,6 1
Authenti_ cation	Au	Base	Multiple Single None	M S N	0,5 0,55 1
Attack Complexity	AC	Base	High Medium Low	H M L	0,5 0,75 1
Exploit_ ability	E	Temporal	Unproven Proof-of-Conc. Functional High Not Defined	U POC F H N	0,85 0,9 0,95 1 1
Report Confidence	RC	Temporal	Unconfirmed Uncorroborated Confirmed Not Defined	UC UR C N	0,9 0,95 1 1

probability calculation. Two new metrics related to a threat-source, Threat Motivation and Threat Capability are employed for the probability calculation.

A novel metric, User Detection (UD), defines the probability of exploits be identified by users as a result of the exploitation side effects at the assets. This metric is calculated from the integrity and availability impacts of the CVEs and can be derived from the underlying CVSS metrics. Confidentiality impacts of CVE exploitations are disregarded since they are usually undetectable by users. UD metric is calculated as depicted in Fig. 4.

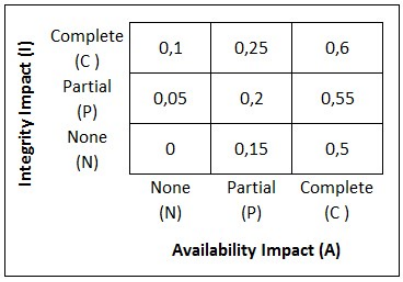

Fig. 4. User Detection (UD) Metric Calculation

Lastly, attack graphs are added as an factor to the risk assessment. Regarding this factor, our assumption is that an attack graph, starting from a threat-source to the target asset, has been generated and provided to us for further processing.

For attack graph-based risk assessment, for each CVE on the assets, firstly interim probabilities without considering the attack graphs are calculated. These interim probabilities are of two types; one including the UD parameter, the other disregarding it. Interim probabilities with UD parameters are used for the calculation of leading probabilities in the attack graph. Interim probability calculations for threat-based-risk assessment is given in (2) and (3). Related metrics employed are described at Table III and Fig. 5.

$$P_{Interim} = TM * TC * AC * Au * E * RC \quad (2)$$

$$P_{InterimWithUD} = TM * TC * AC * Au * E * RC * (1 - UD) \quad (3)$$

TABLE III
ATTACK GRAPH-BASED RISK: LOW LEVEL METRICS FOR PROBABILITY CALCULATION

Metric	Abb.	CVSS	Metric Val.	Abb.	Num. Val.
Threat Motivation	TM	N/A	High Medium Low	H M L	1 0,5 0,3
Threat Capability	TC	N/A	High Medium Low	H M L	Use Fig. 5
Attack Complexity	AC	Base	High Medium Low	H M L	
Authenti-cation	Au	Base	Multiple Single None	M S N	0,5 0,55 1
Exploit_ ability	E	Temporal	Unproven Proof-of-Conc. Functional High Not Defined	U POC F H N	0,85 0,9 0,95 1 1
Report Confidence	RC	Temporal	Unconfirmed Uncorroborated Confirmed Not Defined	UC UR C N	0,9 0,95 1 1
User Detection	UD	N/A	N/A	N/A	Use Fig. 4

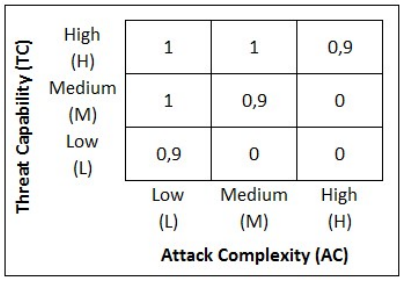

Fig. 5. Threat Capability-Attack Complexity Calculation Matrix

The attack graph-based interim probabilities explained above could be used as the probability of an attacker if he can directly exploit a CVE on the assets. However, if a number of CVEs on an attack graph needs to be exploited first in order to exploit a CVE, the probability for the leading CVEs also needs to be incorporated into the calculation according to the attack graph. Thus, the attack graph-based probability of a CVE can be defined as formulated in (4).

$$P_{AttackGraphBased} = P_{Leading} * P_{Interim} \quad (4)$$

Leading probabilities on an attack graph are calculated by a combination of intersection and union formulas using each CVEs interim probabilities with UD metrics.

As exemplified in Fig. 6, if a particular CVE could only be exploited provided that previous CVEs are also exploited

in the attack graph, the leading probability is calculated by multiplication of each of the CVE probabilities. If we denote interim probabilities with UD metrics by P_i, then the attack graph based probability of CVE_3 can be formulated as depicted in (5) and (6) ($i = 2$ for the example in Fig. 6).

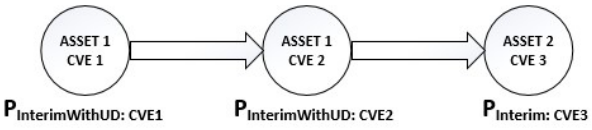

Fig. 6. Attack Graph With Sequential CVEs

$$P_{Leading:CVE_3} = \Pi_i P_i \tag{5}$$

$$P_{AttackGraphBased:CV_3} = P_{Leading:CVE_3} * P_{Interim:CVE_3} \tag{6}$$

As exemplified in Fig. 7, if the attack graph has parallel (alternative) paths leading to a CVE, then the leading probability is calculated by the probabilistic union function. If we denote interim probabilities with UD metrics by P_i, then the attack graph-based probability of CVE_3 can be formulated as depicted in (7) and (8) ($i = 2$ for the example in Fig. 7).

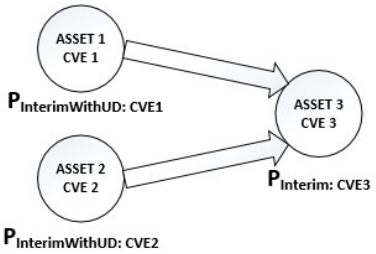

Fig. 7. Attack Graph With Parallel CVEs

$$P_{Leading:CVE_3} = 1 - \Pi_i (1 - P_i) \tag{7}$$

$$P_{AttackGraphBased:CV_3} = P_{Leading:CVE_3} * P_{Interim:CVE_3} \tag{8}$$

For both categories of risk assessment, to calculate the impact of a CVE at an asset, first we calculate the non-remediated impact scores by multiplying the CIA requirements of the assets and the CIA impacts of the vulnerabilities. Then the final impact is calculated by the average value of impact scores multiplied by the remediation level. The range of impact values lie in a scale of (0 to 100). Impact calculation formula is given in (9), (10), (11) and (12). Employed metrics derived from underlying CVSS metrics are described at Table IV.

$$ImpactConfidentiality \rightarrow IC = CR * C \tag{9}$$

$$ImpactIntegrity \rightarrow II = IR * I \tag{10}$$

$$ImpactAvailability \rightarrow IA = AR * A \tag{11}$$

$$Impact = (IC + II + IA)/3 * (1 - RL) \tag{12}$$

TABLE IV
LOW LEVEL METRICS FOR IMPACT CALCULATION

Metric	Abb.	CVSS	Metric Val.	Abb.	Num. Val.
Conf. Impact	C	Base	Complete	C	1
Integ. Impact	I		Partial	P	0,5
Avail. Impact	A		None	N	0
Conf. Req.	CR	Envr.	Low	L	30
Integ. Req.	IR		Medium	M	60
Avail. Req.	AR		High	H	100
			Not Defined	N	100
Remediation Level	RL	Temp.	Official Fix	OF	0,15
			Temporary Fix	TF	0,1
			Work Around	W	0,05
			Unavailable	U	0
			Not Defined	N	0

Lastly, risk is defined as the product of the likelihood of a threat events occurrence and the potential impact should the event occurs, as formulated in (13).

$$Risk = Probability * Impact \tag{13}$$

IV. DEFINITIONS OF HIGH LEVEL RISK METRICS

In this section, we define high level metrics to assess the risk of a system in five categories of views: CVEs, assets, products, threat sources and attack paths. Organizations may fail in risk management when there is only one flat view of risk. High level metrics are useful to gain different views of the risk landscape. Among these high level risk metrics, Risk of a CVE at an Asset is the starting point for the rest of the metrics. High level risk metrics are derived in two ways:

- Nave methods (such as simple sum ups or taking the maximums),
- Probabilistic aggregations of independent events.

The derived metrics that involve summing up of other metrics are in the range of (0 to ∞). For the rest of the metrics the range of values lie in a scale of (0 to 100).

A. CVE Risk Metrics

1) Risk of a CVE at an Asset: This metric shows the risk of a CVE at a specific asset. Base risk of a CVE on an asset can simply be calculated as described in (14), (15) and (16).

$$Risk = Probability * Impact \tag{14}$$

$$Probability = AV * AC * Au * E * RC \tag{15}$$

$$Impact = (IC + II + IA)/3 * (1 - RL) \tag{16}$$

Though there is only one base risk for a CVE on an asset, attack graph-based risk of a CVE on an asset needs to be calculated for each threat source. The calculation for the attack graph-based risk of a CVE at an asset for each threat source is described in (17), (18) and (19).

$$Risk_{ThreatSource} = P_{ThreatSource} * Impact \tag{17}$$

$$P_{ThreatSource} = P_{Leading} * P_{Interim} \tag{18}$$

$$P_{Interim} = TM * TC * AC * Au * E * RC \tag{19}$$

Risk of a CVE on an asset can also be calculated for the case where multiple attack sources might be exploiting the same CVE simultaneously. In this scenario, since the same CVE on an asset is exploited, the impact of the exploitation of the CVE is the same for all the threat sources on that asset. However, each threat source exploits the same CVE with possibly varying probabilities. If we denote these probabilities by P_i, the risks imposed by each threat source can be aggregated as formulated in (20) and (21).

$$Risk = P_{Aggregated} * Impact \tag{20}$$

$$P_{Aggregated} = 1 - \Pi_i(1 - P_i) \tag{21}$$

2) Total Risk Of A CVE At The System: Total risk of a CVE at a system is the sum up of the risks of CVEs at each asset in the system. Though defined as a system level metric, it can be applied to a group of assets as well. For the attack graph-based model, there might be more than one attack graph-based risk value for each threat source. In this case, the aggregated risk of a CVE by multiple threat sources, as described in (20) and (21), is used for summing up.

3) Highest Risk Of A CVE At The System: Highest risk of a CVE at a system is the highest of the risks that a CVE causes at all the assets.

4) Highest Confidentiality, Integrity and Availability Risks At an Asset: In addition to showing the risks of each CVE, we suggest that identification of the highest CIA risks imposed by the CVEs at the assets might also be useful. The need for this metric arises from the fact that impact on one of the CIA factors might be suppressed by the other two factors when the impact is calculated by using all the three factors.

B. Asset And System Risk Metrics

Assets are any computer or network equipment on which software related vulnerabilities might exist. Assets can be grouped in a number of ways (e.g., according to subnets, geographical locations or business functionality).

1) Total Risk at an Asset: Total risk at an asset is the total of the risks of each CVE residing at a given asset. For the attack graph-based model, aggregated risk of a CVE by multiple threat sources, as described in (20) and (21), is used for summing up.

2) Consolidated Risk of an Asset: While calculating the total risk at an asset, we have not set maximum impact values. Thus, if there are multiple probabilities corresponding to multiple CVEs, then it is possible that total risk at an asset is higher than the actual value of that asset if aggregated risk is simply calculated by summing up each risk.

In this section, we define a more elaborate formula to exploit the fact that an asset has a predefined maximum loss value. Thus the total risk should not exceed this maximum. We first note that without loss of generality the following procedure could be applied to confidentiality, integrity and availability risks and the average value of these risks could be calculated at the end. We omit the subscripts of risks for better readability.

We suppose that there are finite number of exploitable CVEs having a nonzero probability applicable to an asset. We define the sample space as the set of all possible outcomes. As an example, consider we have two exploitable CVEs and we name them E_1 and E_2. Thus, the sample space has four elements: $S = (E_1, E_2), (E_1, notE_2), (notE_1, E_2), (notE_1, notE_2)$. We use the term not when that CVE is not exploited in that particular element of the sample space. With this new view on the notion of sample space, we can define our formula to calculate the consolidated risk as in Algorithm 1.

Algorithm 1: Consolidated Risk Algorithm

```
elements ← {(E1, E2), (E1, notE2), (notE1, E2), (notE1, notE2)} ;
p, i, risk_e, consolidatedRisk ← 0 ;
foreach e ∈ elements do
    p ← P(e)
    i ← I(e)
    risk_e ← p * i * (1 − RL)
    consolidatedRisk+ = risk_e
end
```

In Algorithm 1, the probability of each element is calculated using (22). Each element corresponds to a result in which a subset of CVEs is exploited (denoted as ES) and a complementary subset of CVEs is not exploited (denoted as NES).

$$P(e) = \Pi_{i \epsilon ES} P_i \Pi_{j \epsilon NES}(1 - P_j) \tag{22}$$

In Algorithm 1, the impact of each element is calculated by choosing the minimum of either the assets predefined maximum value ($Impact_{max}$) or the sum of the impacts of exploited CVEs, as formulated in (23). Thus, the impact of each element in the sample space is upper bounded by the $Impact_{max}$ value which can be derived from the Table IV.

$$I(e) = min(Impact_{max}, \Sigma_{i \epsilon ES} Impact_i) \tag{23}$$

Example: We provide a toy example to show how consolidated risk of an asset is calculated and how it is different from the total risk at an asset.

Suppose that there are only two vulnerabilities, E_1 and E_2 at a given asset. Probability and impact values of each are as follows: $P(E_1) = 0.8, P(E_2) = 0.9$ and $I(E_1) = 75, I(E_2) = 70$. Suppose further that $Impact_{max} = 100$.

If we calculate the total risk at an asset using the formula as $P(E_1) * I(E_1) + P(E_2) * I(E_2)$, we find its value as 123. This value exceeds $Impact_{max}$.

For the consolidated risk, first we calculate the probability values using (22):

$P(E_1, E_2) = 0.72, P(E_1, notE_2) = 0.08, P(notE_1, E_2) = 0.18, P(notE_1, notE_2) = 0.02$.

Second, we calculate the impact values using (23):

$I(E_1, E_2) = min(100, 75 + 70) = 100, I(E_1, notE_2) = 75, I(notE_1, E_2) = 70, I(notE_1, notE_2) = 0$

Finally, if we suppose $RL = 0$, consolidated risk (CR) of an asset could be calculated using Algorithm 1 as follows:

$CR = 0.72 * 100 + 0.08 * 75 + 0.18 * 70 + 0.02 * 0 = 90.6$

As shown, the value of consolidated risk in this example is smaller than the maximum value of 100, therefore more meaningful than the calculated value of total risk. It could be mathematically proven that consolidated risk could never be larger than $Impact_{max}$. Due to space limitations we leave the proof to the reader.

Up to this point, the given description is for the base risk. However, it could also be used for the attack graph-based model. For this task, first the attack graph-based probability of CVEs by multiple threat sources is calculated. Then, the formulations in (20) and (21) are applied to find the consolidated risk of an asset.

3) Highest Risk at an Asset Group or at the System: Highest risk at an asset group is the consolidated risk of an asset in the group for which the risk is highest. This metric can also be used at the system level.

4) Total Risk for an Asset Group or for the System: Total risk for an asset group or for the system is the sum up of consolidated risks of all the assets in the asset group or in the system. This metric can also be used at the system level.

C. Product Risk Metrics

In our work, products are defined as software which might have any vulnerabilities on them. Products can be put together in any meaningful way (e.g. according to vendors or functionality) to form product groups.

1) Risk of a Product at an Asset: This metric is calculated by aggregating the risks of CVEs at an asset related to a product. The probabilistic aggregation of the risks of related CVEs is figured out as described in (14), (15), (16), (17), (18) and (19). Note that a CVE might be related to more than one product. Thus, only the CVEs related to a product are taken into account only if that product exists on that asset. For the attack graph-based model, aggregated risk of a CVE by multiple threat sources, as described in (20) and (21), is used for summing up.

2) Highest Risk of a Product: Highest risk of a product is the highest of the risks of a product at each asset.

3) Total Risk of a Product: Total risk of a product is the total of the risks of a CVE at each asset.

4) Highest Risk of a Product Group: This metric is the highest of the risks of all the products in a given product group.

5) Total Risk of a Product Group: This metric is the sum up of the total risks of the products in a given product group.

D. Threat Source Risk Metrics

1) Total Risk of a Threat Source: Risk of a threat source is the total of the attack graph-based risks of all the CVEs on the assets exploitable by that threat source.

2) Total Risk of a Threat Source Group: Risk of a threat source group is the sum up of the aggregated risks of CVEs by multiple threat sources as described in (20) and (21).

E. Attack Path Risk Metrics

An attack path can be described as an independent attack scenario from attack source to a target that can be derived from the attack graph [14]. The total risk of an attack path can be calculated by summing up of the attack graph-based risks of each CVE exploited on a given attack by a threat source.

To finalize this section, we argue that the provided extensive list of high level risk metrics enable better decision making for IT systems considering that cyber risks are becoming more complex than ever.

V. RELATED WORK

As described earlier, industry standards such as ISO 27005 and NIST SP 800-30 are high level frameworks for risk assessment with a focus on auditing. They lack sufficient attention to measurement. Thus, they suffer from serious deficiencies as a metrics framework [7]. To address the need for a metrics oriented framework, ISO 27004: Information Security Management-Measurement was developed. However, it focuses on the mechanics of the measurement processes with lack of guidance on which metrics to be used in which circumstance [9].

Another industry standard that might be considered as a panacea for metrics framework need in IT systems is the vulnerability based open risk assessment framework; CVSS [8]. CVSS is very useful in disseminating common metrics of the CVEs in three groups: base, temporal and environmental. However, it suffers mainly from two deficiencies. First, CVSS assesses the risks of single CVEs and does not explain how to assess the risks of system components such as assets, asset groups, products, etc. Second, it disregards both the attack sources and the attack paths for risk calculation. Our model, on the other hand, involves not only the base risk of a system, but also demonstrates the attack graph-based risks. We also measure risks not for only single CVEs but for a collection of CVEs on the assets, products, attack sources and attack paths in a given IT system.

Hubbard and Seiersen [4] advocate to define a set of standard security metrics that are quantifiable and then use them continuously to ensure improvement. However, designed to be a roadmap for establishing cybersecurity risk management, their work does not define or propose a specific cyber security risk assessment methodology for IT systems, which is the focus of our work.

Pendleton et al. [15] explore security metrics systematically based on the attack-defense interactions and propose the following dimensions to categorize systems security metrics: (1) metrics of system vulnerabilities, (2) metrics of defense power, (3) metrics of attack or threat severity, and (4) metrics of situations. However, having a focus on metrics, their work does not discuss a particular risk assessment methodology.

Cheng et al. [10] attempt to improve aggregation of CVSS scores for network risk measurement in two major ways. First, using base scores, they suggest generating dependency relationships with well-defined semantics. Second, they broaden the scope of CVSS standard by aggregating underlying metrics

(Access Vector, Authentication, Access Complexity) of the base scores in three categories (Probabilities, Time and Effort, Skill) to preserve the initial semantics of the metrics. Our work is different than theirs in two ways: First, we stick to the well-established risk formula and define the metrics accordingly in two major types: probability and impact. Second, we also benefit from the temporal CVSS metrics in addition to the base metrics.

Singhal and Ou [13] present a risk assessment model and methodology using CVSS scores and probabilistic attack graphs. With the assumption that an attack graph is given, we present a more comprehensive methodology than their work by employing additional low level metrics and a more detailed discussion and formulation of high level metrics.

Alhomidi and Reed [14] focus on finding the highest risk minimal attack trees using a genetic algorithm. Their work does not define risk metrics and formulations. Since our work focuses on developing a cybersecurity risk assessment methodology, we do not provide an extensive discussion of earlier work on attack graphs. Instead, we refer interested readers to recent work [16] and comprehensive surveys [17] [18].

There are commercial tools that use CVSS scores for network security risk assessment e.g., Skybox [19]. Skybox similarly shows risk of a network in two ways: (1) base CVSS scores for the CVEs on the system. (2) attack graph-based risk of the system. However, as being proprietary, many details in their methodology of risk assessment are unreachable. Unlike Skybox which seems to use CVSS scores as black box inputs, we benefit from the underlying metrics of CVSS to combine them with additional new low level metrics. Then, we define and formulate high level risk metrics on top of low level metrics.

VI. CONCLUSIONS AND FUTURE WORK

In this work, we proposed a quantitative, asset and vulnerability centric cyber security risk assessment methodology for IT systems. We defined both low and high level risk metrics and presented formulas for calculation and aggregation. We used the underlying metrics of CVSS and proposed additional low level metrics. We proposed and discussed high level metrics so that different views of the risk landscape are available for a better decision making. We demonstrated the applicability of our approach on an example system for which the calculations were made by a proof-of-concept program developed in Java language. This open-source software and the results produced can be found at [20].

For the future work, we aim to improve our model in a number of ways. First, dependencies of the impacts of the CVEs on assets can be modeled to improve this work. A dependency defines how exploitation of a CVE affects other assets in the system. A simple example could be the case where unavailability of a DNS server causes availability impacts on other assets. Second, in our work, we assume that all vulnerabilities in the system are already known. As a future work, our risk assessment methodology could be extended by addressing the threats due to zero-day exploits. Lastly, as the database for CVSS 3.0 becomes more complete, we can adapt our work to the CVSS 3.0.

ACKNOWLEDGMENT

This work was supported by The Scientific and Technological Research Council of Turkey (TÜBİTAK), TEYDEB 1501, Grant No: 3160047.

REFERENCES

[1] NIST, "NIST Special Publication 800-30R1: Guide for conducting risk assessments," *NIST Special Publication 800-30R1*, no. September, p. 95, 2012.

[2] D. Kim and M. Gregg, "Why You Need to Conduct Risk Assessment," in *Inside Network Security Assessment: Guarding Your IT Infrastructure*, 2005, p. 312.

[3] S. Elena Ramona, "Advantages and Disadvantages of Quantitative and Qualitative Information Risk Approaches," *Chinese Business Review*, vol. 10, no. 12, pp. 1106–1110, 2011.

[4] D. W. Hubbard and R. Seiersen, *How to Measure Anyting in Cybersecurity Risk*. New Jersey, USA: Wiley, 2016.

[5] Certification Europe, "ISO 27001 Information Security Certification," p. 1, 2014. [Online]. Available: http://certificationeurope.com/iso-27001-information-security/

[6] NIST, "NIST Special Publication 800-37 R1: Guide for Applying the Risk Management Framework to Federal Information Systems," *NIST Special Publication*, vol. 1, no. 1, pp. 800–37, 2010.

[7] A. Jaquith, *Security Metrics: Replacing Fear, Uncertainty, and Doubt*. Boston. MA: Pearson, 2007.

[8] P. Mell, K. Scarfone, and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," *FIRSTForum of Incident Response and Security Teams*, pp. 1–23, 2007.

[9] K. Brotby and G. Hinson, *PRAGMATIC Security Metrics: Applying Metametrics to Information Security*. Boca Raton, FL: Auerbach, 2013.

[10] P. Cheng, L. Wang, S. Jajodia, and A. Singhal, "Aggregating CVSS base scores for semantics-rich network security metrics," *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, pp. 31–40, 2012.

[11] FIRST, "Common Vulnerability Scoring System v3.0: Specification Document," *Forum of Incident Response and Security Teams (FIRST)*, pp. 1–21, 2015.

[12] NIST, "Standards for security categorization of federal information and information systems," *FIPS*, vol. 199, no. February 2004, p. 13, 2004.

[13] A. Singhal and X. Ou, "Security Risk Analysis of Enterprise Networks Using Probabilistic Attack Graphs," *Computer*, p. 24, 2011.

[14] M. Alhomidi and M. Reed, "Attack Graph-Based Risk Assessment and Optimization Approach," *International Journal of Network Security & Its Applications (IJNSA)*, vol. 6, no. 3, pp. 31–43, 2014.

[15] M. Pendleton, R. Garcia-Lebron, and S. Xu, "A Survey on Security Metrics," *arXiv preprint arXiv:1601.05792*, vol. 49, no. 4, 2016.

[16] M. U. Aksu, M. H. Dilek, E. . Tatl, K. Bicakci, and M. Ozbayoglu, "Automated Generation Of Attack Graphs Using NVD," in *submitted for publication (24th ACM Conference on Computer and Communications Security)*, 2017.

[17] R. Lippmann and K. Ingols, "An annotated review of past papers on attack graphs," *(No. PR-IA-1). Massachusetts Inst. Of Tech. Lexington Lincoln Lab.*, no. March, 2005.

[18] V. Shandilya, C. B. Simmons, and S. Shiva, "Use of attack graphs in security systems," *Journal of Computer Networks and Communications*, vol. 2014, 2014.

[19] "Skybox Security." [Online]. Available: https://www.skyboxsecurity.com/

[20] "Risk Assessment Model: PoC Coding in Java." [Online]. Available: https://gitlab.com/stm-public/risk-assessment-framework-model