

Composite metrics for network security analysis

AUTHOR(S)

Simon Enoch Yusuf, Jin B Hong, Mengmeng Ge, Dong Seong Kim

PUBLICATION DATE

01-01-2018

HANDLE

10536/DRO/DU:30131764

Downloaded from Deakin University's Figshare repository

Deakin University CRICOS Provider Code: 00113B

Composite Metrics for Network Security Analysis

Simon Enoch Yusuf, Jin B. Hong, Mengmeng Ge
and Dong Seong Kim

Department of Computer Science and Software Engineering,
University of Canterbury, Private Bag 4800,
Christchurch, New Zealand
E-mail: simon.yusuf@pg.canterbury.ac.nz; {jho102, mge43}@uclive.ac.nz;
dongseong.kim@canterbury.ac.nz

Received 28 June 2016; Accepted 16 February 2017;
Publication 25 February 2017

Abstract

Security metrics present the security level of a system or a network in both qualitative and quantitative ways. In general, security metrics are used to assess the security level of a system and to achieve security goals. There are a lot of security metrics for security analysis, but there is no systematic classification of security metrics that is based on network reachability information. To address this, we propose a systematic classification of existing security metrics based on network reachability information. Mainly, we classify the security metrics into host-based and network-based metrics. The host-based metrics are classified into metrics "without probability" and "with probability", while the network based metrics are classified into "path-based" and "non-path based". Finally, we present and describe an approach to develop composite security metrics and it's calculations using a Hierarchical Attack Representation Model (HARM) via an example network. Our novel classification of security metrics provides a new methodology to assess the security of a system.

Keywords: Attack Graphs, Cyber Security, Graphical Security Model, Security Assessment, Attack Trees.

Journal of Software Networking, 137–160.
doi: 10.13052/jsn2445-9739.2017.007
© 2017 *River Publishers. All rights reserved.*

1 Introduction

Researchers from research institutions, governments and industries have been working on developing and distributing security metrics. For instance, the Center for Internet Security (CIS) [3] proposed and categorised security metrics into management, technical and operational metrics. The National Institute of Standards and Technology (NIST) [2] proposed nine security metrics into implementation, effectiveness/efficiency and impact. Others such as Idika and Bhargava [15] proposed and classified security metrics into decision, assistive and so on. Most of these efforts to categorise and classify security metrics are based on the target audience and personal intuitions. Therefore, it is important to develop a systematic classification of security metrics that is based on network reachability information. There are a number of security metrics which are used for network security assessment [15, 30, 32, 39, 40]. But none of them are capable of representing the overall security level of the network [19]. Thus it is important we combine different security metrics to present and analyse the diverse facet of the security posture.

In this paper, we classify the existing security metrics based on network reachability information, and describe an approach to develop new security metrics by combining the existing security metrics. Our novel classification provides a new methodology to assess the security of a system. It also provides insight as to how and when a security metric should be used. The main contributions of this paper are:

- to classify existing cyber security metrics;
- to perform security analysis using the existing security metrics;
- to describe an approach to developing composite security metrics; and
- to formally define the composite security metrics.

The rest of the paper is organised as follows. Section 2 introduces related work on existing classification of security metrics. In Section 3, we present a novel classification of the existing security metrics. In Section 4, we describe and analyse the security of an example network using existing security metrics. In Section 5, we present our new composite security metrics with examples. And finally, we conclude the paper and outline the future work in Section 6.

2 Related Work

There are a few research on the classification of security metrics. Most classification methods are based on organisation's point of view [37]. For instance, Savola [36] proposed three categories of security metrics; namely,

(i) business-level security metrics, (ii) metrics for information security management (ISM) in organisations, and (iii) dependability and trust metrics for products, systems and services. The business-level security metrics are business goals directed and are used for cost-benefit security analysis in organisations. The information security management metrics are used to evaluate the ISM security controls, plans and policies, and are divided into three subcategories (i.e., management, operational and information system technical security metrics). The dependability and trust metrics are used to assess the organisation's trust, relationships and dependability issues [1]. In general, this classification only addresses the security needs of companies that produce information and telecommunication technology products, systems or services.

Vaughn *et al.* in [38] presented two categories of security metrics (organisational security metrics and metrics for technical target assessment). The organisational security metrics assess the organisation's security assurance status (the metrics in this category include security effectiveness, operational readiness for security incidents and information assurance program development metric). The metrics for technical target assessment are used to assess the security capabilities of a technical system (it is further divided into metrics for strength assessment and metrics for weakness assessment [38]). This classification is tailored towards an organisation's needs.

Pendleton *et al.* [31] classified security metrics into four categories, namely: metrics for measuring the system vulnerabilities, metrics for measuring the defences, metrics for measuring the threats, and metrics for measuring the situations. The metrics for measuring vulnerabilities are intended to quantify the enterprise and computer systems vulnerabilities through their user's password, software vulnerabilities, and the vulnerabilities of the cryptographic keys they use. The metrics for measuring defences is aimed to quantify the countermeasure deployed in an enterprise via the effectiveness of blacklisting, the ability of attack detection, the effectiveness of software diversification, and the overall effectiveness of these countermeasures. The metrics for measuring threats are aimed to assess the threats against an enterprise through the threat of zero-day attacks, the power of individual attacks and the sophistication of obfuscation. And the metrics for measuring the situations aims to assess situations via security investments, security states and security incidents. This classification is centred on the perspective between attackers and defenders in enterprise systems. Other classifications provided by industries such as the NIST [2], the CIS [3] and the Workshop on Information Security System Scoring and Ranking are exclusively geared towards cyber defence administrations and operations [31].

To the best of our knowledge, there is no previous work on the classification of security metrics based on the network reachability information. Here, we focus on classifying existing security metrics based on network reachability information and propose an approach to develop new set of cyber security metrics by combining the existing metrics.

3 Classification of Security Metrics

Based on network reachability information, we mainly classify security metrics into two types: host-level metrics and network-level metrics, as shown in Figure 1.

The host-level metrics do not use any network level information (e.g., reachability, protocols, *etc*) whereas the network-level metrics take into account network structure, protocol and reachability information to quantify the security of a system. We describe the host-level metrics in Section 3.1 and the network-level metrics in Section 3.2, respectively.

3.1 Host-based Security Metrics

The host-level metrics are used to quantify the security level of individual hosts in a network. We further classify the host-level metrics into two types: "without probability" and "with probability". The reasons for this classification are: (i) sometimes it is infeasible to find a probability value for an attack, and (ii) some analysis and optimisation can be done with or without probability assignments as described in [34].

3.1.1 Metrics without probability values

We summarise the metrics "without probability" in Table 1. Examples of metrics without probability values are attack impact, attack cost, structural important measured [33], mincut analysis [33], mean-time-to-compromise

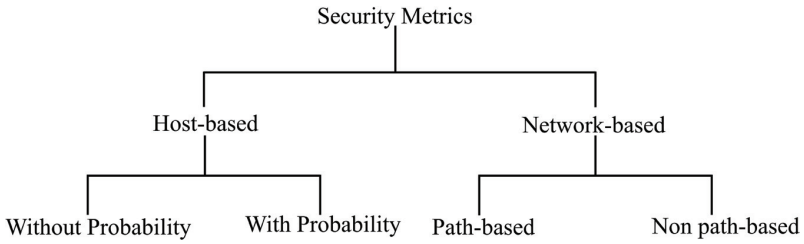


Figure 1 Classification of security metrics.

Table 1 Description of metrics without probability values

Metrics	Description
Attack Cost [33]	is the cost spent by an attacker to successfully exploit a vulnerability (i.e., security weakness) on a host.
Attack Impact [13]	is the quantitative measure of the potential harm caused by an attacker to exploit a vulnerability.
Mean-time-to-Compromise (MTTC) [10, 20]	is used to measure how quickly a network can be penetrated. This type of metrics produces time values as end results.
Structural Important Measure [33]	is used to qualitatively determine the most critical event (attack, detection or mitigation) in a graphical attack model. This metric is useful when the probability of event such as attack, detection or mitigation are unknown.
Mean-Time-to-Recovery (MTTR) [16]	is used to assess the effectiveness of a network to recovery from an attack incidents. It is defined as the average amount of time required to restore a system out of attack state. The shorter the time, the less impact is the attack on the overall performance of the network.
The Return on Attack [4]	is defined as the gain the attacker expects from successful attack over the losses he sustains due to the countermeasure deployed by his target. This security metric is from the attacker perspective and it used by organisations to evaluate the effectiveness of a countermeasure in discouraging a certain type of intrusion attempts [4].

(MTTC) [10, 20], mean-time-to-recovery (MTTR) [16], Mean-Time-to-First-Failure (MTFF) [35], Mean-Time-to-Breach (MTTB) [17], The return on investment [4], The return on attack [4], *etc*.

3.1.2 Metrics with probability values

Conversely, the security metrics with probability include probability security metric [39], Common Vulnerability Scoring System (CVSS) metrics [6] *etc*. An attack graph (AG) is an acyclic directed graph to represent all possible ways for an attacker to reach a target vulnerability. Wang *et al.* [39] proposed an AG-based security metric that incorporates the likelihood of potential

Table 2 Description of metrics with probability values

Metrics	Description
Probability of vulnerability exploited [8]	is used to assess the likelihood of an attacker exploiting a specific vulnerability on a host. This takes into account the severity of the host vulnerability.
Probability of attack detection [33]	is used to assess the likelihood of a countermeasure to successfully identify the event of an attack on a target.
Probability of host compromised [11]	is used to assess the likelihood of an attacker to successfully compromise a target
CVSS [6, 23]	is an industry standard used to assess the severity of computer vulnerabilities. Details of the CVSS probability is provided in [29].

multi-step attacks combining multiple vulnerabilities in order to reach the attack goal. We summarise the metrics with probability in Table 2.

3.2 Network-based Security Metrics

This category of metrics uses the structure of a network to aggregate the security property of the network. We further classify these metrics into two types: path based and non-path based metrics (according to the use of path information).

3.2.1 Non-path based metrics

In non-path based metrics, the structure and attributes of a network are not considered; instead, the security of a network is quantified regardless of the network structure. One example of this type of metrics is Network Compromise Percentage (NCP) metric [22]. The NCP metric is defined in Table 4. This metric indicates the percentage of network assets an attacker can compromise. The aim of the NCP metric is to minimise this percentage. Another example is a set of vulnerabilities that allows an attacker to use them as entry points to a network. For instance, web-services running on a host could be the very first targets for an attacker to compromise. The weakest adversary (WA) metric is also a network based metric that is use to assess the security of a network. In the WA metric, a network configuration that is vulnerable to a stronger set of attribute is define as more secure than a network configuration that is vulnerable to a weaker set of initial attacker attributes [30].

3.2.2 Path based metrics

Path based metrics use the reachability information of a network (for example, reachability between hosts, shortest path from a host X to a host Y, and so on) to quantify the security level of the network. Wesummarise some of these metrics in Table 3, which include Shortest Path (SP)

Table 3 Description of path based metrics

Metrics	Description
Attack Shortest Path [27, 32]	is the smallest distance from the attacker to the target. This metric represents the minimum number of hosts an attacker will use to compromise the target host.
Number of Attack Paths [27]	is the total number of ways an attacker can compromise the target. The higher the number, the less secure the network.
Mean of Attack Path Lengths [21]	is the average of all path lengths. It gives the expected effort that an attacker may use to breach a network policy.
Normalised Mean of Path Lengths [15]	This metric represents the expected number of exploits an attacker should execute in order to reach the target.
Standard Deviation of Path Lengths [15]	is used to determine the attack paths of interest. A path length that is two standard deviations below the mean of path length metric is considered the attack paths of interest and can be recommended to the network administrator for monitoring and consequently for patching [15].
Mode of Path Lengths [15]	is the attack path length that occurs most frequently. The Mode of Path Lengths metric suggests a likely amount of effort an attacker may encounter.
Median of Path Lengths [15]	this metric is used by network administrator to determine how close is an attack path length to the value of the median path length (i.e. path length that is at the middle of all the path length values). The values that falls below the median are monitored and considered for network hardening [15].
Attack Resistance Metric [40]	is use to assess the resistance of a network configuration based on the composition of measures of individual exploits. It is also use for assessing and comparing the security of different network configurations [40].

Table 4 Description of non-path based metrics

Metrics	Description
Network Compromise Percentage [22]	is the metric that quantifies the percentage of hosts on the network on which an attacker can obtain an user or administration level privilege.
Weakest Adversary [30]	is used to assess the security strength of a network in terms of the weakest part of the network that an attacker can successfully penetrate.
Vulnerable Host Percentage [18]	is used to assess the overall security of a network. This metric quantifies the percentage of hosts with vulnerability on a network. The higher the metric value, the less is the security level of the network.

metrics [32], Number of Paths (NP) metrics [27], Mean of Path Length (MPL) metrics [21], Normalised Mean of Path Lengths (NMPL) Metrics [15], Standard Deviation of Paths Lengths (SDPL) Metrics [15], Mode of Path Lengths (MoPL) Metrics [15] and Median of Path Lengths (MePL) Metrics [15].

4 Network Configurations and System Model

The example network is shown in Figure 2. The network consists of two firewalls with an attacker located outside the network. Here, the firewall 1 is use to allow secure connections from the Internet to the hosts in the network while firewall 2 is use to allow secure connections to the database (i.e., h_7). We assume the goal of the attacker is to compromise the database. We denote hosts in the network as h_i, where $i = 1, 2, 3\ldots, n$ (a unique identifier for each host in the network). Table 6 shows the firewall rules used for the example network. For simplicity, we selected only one vulnerabilities for each host in the network from the Common Vulnerabilities and Exposures (CVE) [6] which we list in Table 7.

We use the example network and existing security metrics to perform security assessment via the Hierarchical Attack Representation Model (HARM) [14]. We describe the HARM and assumptions of the example network in Section 4.1 and Section 4.2, respectively.

The example network has a finite set of hosts H and a finite set of vulnerabilities *V*. The following notations are used for the security assessment.

Table 5 Notations for the security assessment

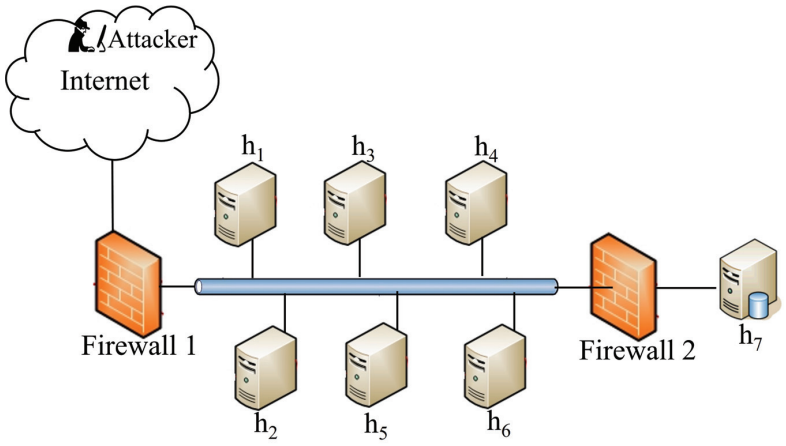
Notation	Meaning
AP	is all possible paths from an attacker to a target
ap	is an attack path which includes a sequence of hosts
f	is a function that identifies the length of the attack path that occurs most frequently
ac_h	is the minimum cost spent by an attacker who successfully compromises the host *h*
aim_h	is the maximum potential loss caused by an attacker who successfully compromises the host *h*
pr_h	is the probability of an attacker to successfully compromise the host *h*
ac_{ap}	is the minimum cost spent by an attacker who successfully compromises an *ap*
aim_{ap}	is the maximum potential loss caused by an attacker who successfully compromises an *ap*
pr_{ap}	is the probability of an attacker to successfully compromise an *ap*
ap_{ex}	is the attack path that an attacker is attempting to exploit e_x
as_h	is the asset value associated with a host *h*
s_v	is the set of vulnerable hosts

- A graphical security model – HARM denoted as *GSM*
- Each host $h \in H$ has a name h_{name}, a vulnerability $v \in V$ and a set of security metrics $h_{metrics} \subseteq \{p_h, iam_h, ac_h, mttc_h, as_h\}$.
- Each vulnerability $v \in V$ has a name v_{name}.
- Each attack path $ap \in AP$ has an index ap_{index}.

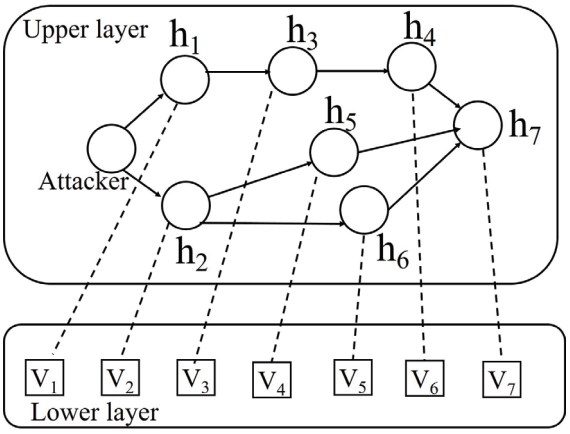
4.1 The HARM

We use the HARM to analyse the network security. The HARM is a two-layer model in which the upper layer (AG) represents the network reachability information and the lower layer (AT) represents the vulnerability information.

We defined the AT [9] for HARM as a 5-tuple $at = (A, B, c, g, root)$. Here, *A* is a set of components which are the leaves of *at* and *B* is a set of gates which are the inner nodes of *at*. We require $A \cap B = \emptyset$ and $root \in A \cup B$. Function c: $B \rightarrow \mathcal{P}(A \cup B)$ describes the children of each inner node in *at* (we assume there are no cycles). Function g: $B \rightarrow \mathcal{P}\{AND, OR\}$ describes the type of each gate. The representation of the AT at_h associated to the host $h \in H$ is given as at_h: $A \subseteq h_{vuls}$ (where *vuls* is the host vulnerability). This means that the vulnerabilities of a node are combined using *AND* and *OR* gates.



(a) Example Network.



(b) HARM of the Example Network.

Figure 2 An example network and the HARM.

We defined the AG for HARM [9] as a directed graph $ag = (N, E)$ where N is a finite set of components and $E \subseteq N \times N$ is a set of edges between components.

The HARM of the example network is shown in Figure 2(b). Other graphical security models such as those suggested by Noel and Jajodia [25] and Ou *et al.* [28] can also be used.

Table 6 Example network: firewall rules

Host	Accept Traffic From
h_1	Internet
h_2	Internet
h_3	h_1
h_4	h_3
h_5	h_2
h_6	h_2
h_7	h_4, h_5, h_6

4.2 Assumptions for the Example Network

We make the following assumptions for the example network:

- An attacker knows the (or has knowledge of) reachability information from the attacker to the target (that is h_7).
- Each host has only one vulnerability but more vulnerabilities can be modelled as in the work [12, 13].
- Exploiting a vulnerability grants the attacker the root privilege of the host.
- The attacker uses vulnerability scanners such as Nessus [7], Nmap [24], *etc* to discover all the network vulnerabilities.

4.3 Security Analysis of the Example Network

We use existing security metrics to assess the security of the example network. For simplicity, we selected a few vulnerabilities from the Common Vulnerabilities and Exposures (CVE) [6] which we list in Table 7.

In Table 7, the host-based metrics "without probability" values; attack cost and attack impact have metric value of 5.50 and 4.30 for target host h_7, respectively. These metrics present the minimum cost and the potential

Table 7 List of vulnerabilities

h_{name}	v_{name}	*CVE–ID*	*CVSS BS*	pr_h	aim_h	ac_h	as_h
h_1	v_1	CVE–2016–2386	7.5	0.75	7	8	40
h_2	v_2	CVE–2016–2040	3.5	0.35	4	4.2	21
h_3	v_3	CVE–2016–0059	4.3	0.43	5	5.2	25
h_4	v_4	CVE–2015–7974	2.1	0.21	3	3.5	17.5
h_5	v_5	CVE–2015–2542	9.3	0.93	9	9.2	46
h_6	v_6	CVE–2014–2706	7.1	0.71	6.5	7.5	37.5
h_7	v_7	CVE–2013–2035	4.4	0.44	4.3	5.5	27.5

loss for the attacker to successfully compromise a host h_7, respectively. The probability of attack success metric (i.e., a metric "with probability") is – 0.44. This metric presents the probability that an attacker will successfully exploit the host h_7. The lower the metric value, is the lower the chances that the attacker will succeed in exploiting the target host.

To calculate the network base metrics, we consider a set of all attack paths *AP* (i.e. $ap_1 = (h_1, h_3, h_4, h_7), ap_2 = (h_2, h_5, h_7)$, and $ap_3 = (h_2, h_6, h_7)$) for a given target, h_7. We compute the network based metrics in Table 8 and Table 9.

In Table 8, the value of the shortest path metric is 3. Based on this metric, an administrator can prioritise the network hardening measure by patching vulnerabilities along the shortest path – in this case, it is the attack path ap_2 and ap_3. The number of paths (NP) metric which also yield the value 3.00 indicates the security strength of the network. In the NP metric, the higher the paths number is the lower is the security level. The mean of paths length yield 3.30. This security metrics show the overall network security level. In the mean of path lengths metric, the HARM with higher metric value is recorded as less secure. The standard deviation of path lengths is 0.47. According to this metric, the path length that is two standard deviations below

Table 8 Metrics Values for "path based metrics"

Metrics Name	Formulae	Value
Shortest Attack Path	$SP(GSM) = \min_{ap \in AP} \lvert ap \rvert$	3.00
Number of Attack Paths	$NP(GSM) = \lvert AP \rvert$	3.00
Mean of Attack Path Lengths	$MPL(GSM) = \sum_{\frac{ap \in AP}{NP(GSM)}} \lvert ap \rvert$	3.30
SDPL	$SDPL(GSM) = \sqrt{\frac{\sum_{ap \in AP} (\lvert ap \rvert - MPL(GSM))^2}{NP(GSM)}}$	0.47
Mode of Path Lengths	$MoPL(GSM) = f_{ap \in AP} (\lvert ap \rvert)$	3.00
Attack Resistance	$R(e_i) = \begin{cases} \frac{r(e_i) + R(e_j)}{} & \text{conjuctive} \\ r(e_i) + \frac{1}{R(e_k)^{-1} + R(e_i)^{-1}} & \text{disjunctive} \end{cases}$	8.81

Table 9 Metrics values for "non-path based metrics"

Metrics Name	Formulae	Value
Network Compromise Percentage	$NCP(GSM) = 100 \times \frac{\sum_{h \in ap_{ex}} as_h}{\sum_{h \in AP} as_h}, \quad ap_{ex} \in AP$	51.23%
Vulnerable Host Percentage	$VHP(GSM) = 100 \times \frac{\sum_{h \in s_v} h}{\sum_{h \in AP_v} h}, \quad s_v \in AP$	100%

the mean of path lengths metric is considered to be the attacker's path of interest and regarded as vulnerabilities in hosts along the path are recommended for patching. In this case the ap_2 and ap_3 are both two standard deviation below the MPL metric (their two standard deviation value is –0.64 for both metrics).

To compute the attack resistance metric, two basic operators (disjunctive and conjunctive) described in Wang *et al.* [40] are used. We compute the attack resistance metric based on the equation provided by Idika [26]. In the equation, the function *r* represents the difficulty associated with an exploit e_m. *R* represent the cumulative resistance of an exploit e_m by taking into account all resistance values for ancestors of e_m. We use each host vulnerability value as the exploit value. In our calculation, the attack resistance value is 8.81. This metric value indicates the network security level and the ability of the network configuration to resist attack.

In Table 9, we compute the NCP metric. The NCP security metric is for an AG that is not target oriented. In the NCP computation, we assume the attacker is attempting to compromise the set of machines on ap_1. In our computation, the NCP metric yields a value of 51.23%. In the NCP metric the more machines are compromised, the higher the NCP value. Hence, the goal of the administrator is to reduce the NCP value. The vulnerable host percentage metric yield a value of 100%. This is because all host in our example network has one vulnerability. This security metric is used to compute the percentage of host on a network that have at least one vulnerability.

5 Composite Security Metrics

We propose an approach to develop new set of cyber security metrics called *composite security metrics*. In these metrics, we combine individual metrics to create a new metric (for example, we can combine attack impact and attack

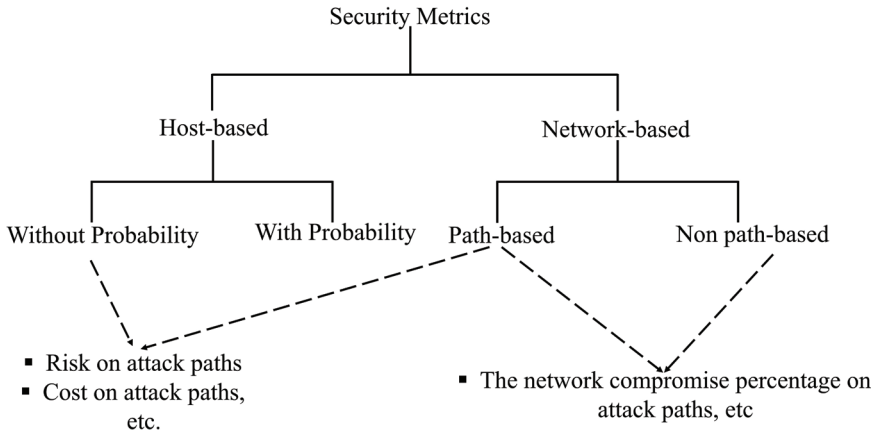


Figure 3 Examples of composite security metrics.

path metric to form the impact on attack path metric, see Figure 3 for more examples). We will use the example network in Figure 2 to perform security analysis using the composite security metrics. We demonstrate our proposed composite metrics using four examples: (i). Impact on attack paths (ii). Risk on attack paths (iii). Return on attack paths (iv). Probability of attack success on paths.

5.1 Impact on Attack Paths

The native metric (as one of the path-based metrics) used to create the impact of paths is attack paths. We combine the attack path metrics with the impact of each host in the path. We define the impact on attack path as the cumulative quantitative measure of potential harm in an attack path. We denote the metric as *AIM* and calculate it using Equations (3) and (4). The host attack impact is calculated by Equation (2). The network-level value *AIM* is then given by Equation (4).

$$aim_b = \begin{cases} \sum\limits_{a \in c(b)} aim_a, & \substack{b \in B \\ g(b)=AND} \\ \max\limits_{a \in c(b)} aim_a, & \substack{b \in B \\ g(b)=OR} \end{cases} \tag{1}$$

$$aim_h = aim_{root} \tag{2}$$

$$aim_{ap} = \sum_{h \in ap} aim_h, \quad ap \in AP \tag{3}$$

$$AIM = \max_{ap \in AP} aim_{ap} \tag{4}$$

The impact on path metric can reveal the impact of damage associated with each attack path. A security administrator can use this metric to determine which path to patch first. For instance, hosts in the path with the highest impact value can be considered as the prioritised set of hosts to patch.

Using the example network, we use all the possible AP from Figure 2 to compute the impact of path metrics.

$$\begin{aligned} aim_{ap_1} &= aim_{h_1} + aim_{h_3} + aim_{h_4} + aim_{h_7} \\ &= 7 + 5 + 3 + 4.3 \\ &= 19.3 \\ aim_{ap_2} &= aim_{h_2} + aim_{h_5} + aim_{h_7} \\ &= 4 + 9 + 4.3 \\ &= 17.3 \\ aim_{ap_3} &= aim_{h_2} + aim_{h_6} + aim_{h_7} \\ &= 4 + 6.5 + 4.3 \\ &= 14.8 \end{aligned}$$

The AIM of the example network is 19.3. More detail of how to get the CVSS impact values can be found in [5].

5.2 Risk on Attack Paths

The Risk on attack paths is defined as the expected value of the impact on an attack path. It is computed as the summation of the product of the probability of attack success pr_h and the amount of damage aim_h h belonging to an attack path *ap*. The metric is denoted as *R* and calculate it using Equation (8). The host risk metric is defined by Equation (6). The network-level value *R* is then given by Equation (8).

$$r_b = \begin{cases} \sum\limits_{a \in c(b)} pr_a \times aim_a, & \substack{b \in B \\ g(b) = AND} \\ \max\limits_{a \in c(b)} pr_a \times aim_a, & \substack{b \in B \\ g(b) = OR} \end{cases} \tag{5}$$

$$r_h = r_{root} \tag{6}$$

$$r_{ap} = \sum_{h \in ap} pr_h \times aim_h, \qquad ap \in AP \tag{7}$$

$$R = \max_{ap \in AP} r_{ap} \tag{8}$$

We compute the risk of paths metric for all the possible attack paths as follows:

$$\begin{aligned} r_{ap_1} &= pr_{h_1} \times aim_{h_1} + pr_{h_3} \times aim_{h_3} + pr_{h_4} \times aim_{h_4} + pr_{h_7} \times aim_{h_7} \\ &= (0.75 \times 7) + (0.43 \times 5) + (0.21 \times 3) + (0.44 \times 4.3) \\ &= 9.92 \\ r_{ap_2} &= pr_{h_2} \times aim_{h_2} + pr_{h_5} \times aim_{h_5} + pr_{h_7} \times aim_{h_7} \\ &= (0.35 \times 4) + (0.93 \times 9) + (0.44 \times 4.3) \\ &= 11.66 \\ r_{ap_3} &= pr_{h_2} \times aim_{h_2} + pr_{h_6} \times aim_{h_6} + pr_{h_7} \times aim_{h_7} \\ &= (0.35 \times 4) + (0.71 \times 6.5) \times (0.44 \times 4.3) \\ &= 7.91 \end{aligned}$$

This metric shows the level of risk associated with each attack path. From our computed example HARM, the attack path ap_2 (it's risk is 11.66) is considered as the path with the highest risk.

5.3 Return on Attack Paths

The return on attack [4] is a metric used to quantify the benefit for the attacker. A return on attack paths computes the benefit for an attacker when the attacker successfully exploits all the vulnerabilities on a particular attack path. From the defender's point of view, the network administrator can use this metric to reduce the attacker's benefit by patching vulnerabilities on the path(s) with a high value of ROA. We denote the metric as *ROA* and it is calculated using Equation (12). The host return on attack metric is given by Equation (10). The network-level value *ROA* is then given by Equation (12).

$$roa_b = \begin{cases} \sum\limits_{a \in c(b)} \dfrac{pr_a \times aim_a}{ac_a}, & \substack{b \in B \\ g(b)=AND} \\ \max\limits_{a \in c(b)} \dfrac{pr_a \times aim_a}{ac_a}, & \substack{b \in B \\ g(b)=OR} \end{cases} \tag{9}$$

$$roa_h = roa_{root} \tag{10}$$

$$roa_{ap} = \sum_{h \in ap} \frac{pr_h \times aim_h}{ac_h}, \qquad ap \in AP \tag{11}$$

$$ROA = \max_{ap \in AP} \ roa_{ap} \tag{12}$$

We show how to compute return on attack paths below:

$$\begin{aligned}
roa_{ap_1} &= \frac{pr_{h_1} \times aim_{h_1}}{ac_{h_1}} + \frac{pr_{h_3} \times aim_{h_3}}{ac_{h_3}} + \frac{pr_{h_4} \times aim_{h_4}}{ac_{h_4}} + \frac{pr_{h_7} \times aim_{h_7}}{ac_{h_7}} \\
&= \frac{0.25 \times 7}{8} + \frac{0.57 \times 5}{5} + \frac{0.79 \times 3}{3.5} + \frac{0.56 \times 4.3}{5.5} \\
&= 1.91 \\
roa_{ap_2} &= \frac{pr_{h_2} \times aim_{h_2}}{ac_{h_2}} + \frac{pr_{h_5} \times aim_{h_5}}{ac_{h_5}} + \frac{pr_{h_7} \times aim_{h_7}}{ac_{h_7}} \\
&= \frac{0.65 \times 4}{4.2} + \frac{0.07 \times 9}{9.2} + \frac{0.56 \times 4.3}{5.5} \\
&= 1.12 \\
roa_{ap_3} &= \frac{pr_{h_2} \times aim_{h_2}}{ac_{h_2}} + \frac{pr_{h_6} \times aim_{h_6}}{ac_{h_6}} + \frac{pr_{h_7} \times aim_{h_7}}{ac_{h_7}} \\
&= \frac{0.65 \times 4}{4.2} + \frac{0.29 \times 6.5}{7.5} + \frac{0.56 \times 4.3}{5.5} \\
&= 1.30
\end{aligned}$$

Return on attack paths quantifies the network security level from the attacker's perspective. From the example network scenario, the attack path ap_1 with metrics value 1.91 has the highest benefit to the attacker.

5.4 Probability of Attack Success on Paths

The probability of attack success on paths is developed by combining path and probability of attack success. The probability of attack success on paths represents the chances of an attacker successfully reaching the target through an attack path. It is calculated by the Equation (16). The host attack success probability is defined by Equation (14). We denote probability of attack success on paths as *Pr*. The network-level value *Pr* is then given by Equation (16).

$$pr_b = \begin{cases} \prod\limits_{a \in c(b)} pr_a, & \substack{b \in B \\ g(b) = AND} \\ 1 - \prod\limits_{a \in c(b)} (1 - pr_a), & \substack{b \in B \\ g(b) = OR} \end{cases} \tag{13}$$

$$pr_h = pr_{root} \tag{14}$$

$$pr_{ap} = \prod_{h \in ap} pr_h, \quad ap \in AP \tag{15}$$

$$pr = \max_{ap \in AP} pr_{ap} \tag{16}$$

We show how to compute the probability of attack success on paths below:

$$\begin{aligned} pr_{ap_1} &= pr_{h_1} \times pr_{h_3} \times pr_{h_4} \times pr_{h_7} \\ &= 0.75 \times 0.43 \times 0.21 \times 0.44 \\ &= 0.03 \\ pr_{ap_2} &= pr_{h_2} \times pr_{h_5} \times pr_{h_7} \\ &= 0.35 \times 0.93 \times 0.44 \\ &= 0.14 \\ pr_{ap_3} &= pr_{h_2} \times pr_{h_6} \times pr_{h_7} \\ &= 0.35 \times 0.71 \times 0.44 \\ &= 0.11 \end{aligned}$$

In this scenario, ap_2 with metric value 0.14 has the highest probability of a successful attack and therefore it is the *Pr*. The closer the *Pr* value is to 1, the higher is the likelihood that an attacker will succeed in exploiting the target.

6 Conclusions and Future Work

In this paper, we have described the existing security metrics for cyber security assessment. We have used the network structure and reachability information to classify the existing metrics into host and network based security metrics. We also use the existing security metrics to carry out security analysis. In addition, we described an approach to developing composite security metrics and finally, we formally defined some composite security metrics.

Our classification of security metrics does not capture dynamic security metrics. Thus, we need to incorporate the dynamic security metrics into the proposed classification.

Acknowledgement

This paper was made possible by Grant NPRP 8-531-1-111 from Qatar National Research Fund (QNRF). The statements made herein are solely the responsibility of the authors.

References

[1] A. Avizienis, J. C. Laprie, B. Randell, and C. Landwehr. (2004). Basic concepts and taxonomy of dependable and secure computing. *IEEE Trans. Dependable Secure Comput.* 1, 11–33.

[2] C. Barker. (2007). *NIST Security Measurement NIST SP 800-55 Revision 1.* Available at: http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2007-09/Barker_ISPAB_Sept2007-SP800-55R1.pdf [accessed February 20, 2016].

[3] CIS. (2010). *The Center for Internet Security: Security Metrics*. Available at: https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf [accessed February 20, 2016].

[4] M. Cremonini and P. Martini. (2005). "Evaluating information security investments from attackers perspective: the return-on-attack (ROA)," in *Proceedings of the Fourth Workshop on the Economics of Information Security*.

[5] CVSS. (2016). *CVSS Calculator.* Available at: https://nvd.nist.gov/CVSS-v2-Calculator/CVSS-v2-Equations [accessed February 27, 2016].

[6] CVSS. (2016). *Forum for Response and Security Team.* Available at: https://www.first.org/cvss [accessed February 3, 2016].

[7] R. Deraison. (2016). *Nessus Scanner.* Available at: http://nmap.org/index.html [accessed February 3, 2016].

[8] K. A. Edge. (2007). *A Framework for Analyzing and Mitigating the Vulnerabilities of Complex Systems via Attack and Protection Trees*. Ph.D. thesis, Air Force Institute of Technology, Wright Patterson AFB, OH.

[9] M. Ge, J. B. Hong, W. Guttmann, and D. S. Kim. (2017). A framework for automating security analysis of the internet of things. *J. Netw. Comput. Appl.* 83, 12–27.

[10] M. Ge and D. S. Kim. (2015). "A framework for modeling and assessing security of the internet of things," in *Proceedings 21st International Conference on Parallel and Distributed Systems (ICPADS)*, (Rome: IEEE), 776–781.

[11] J. Homer, S. Zhang, X. Ou, D. Schmidt, Y. Du, S. R. Rajagopalan, and A. Singhal. (2013). Aggregating vulnerability metrics in enterprise networks using attack graphs. *J. Comput. Secur.* 21, 561–597.

[12] J. Hong and D. S. Kim. (2012). "HARMs: hierarchical attack representation models for network security analysis," in *Proceedings of the 10th Australian Information Security Management Conference on SECAU Security Congress (SECAU 2012)*, Perth, WA.

[13] J. B. Hong. (2015). *Scalable and Adaptable Security Modelling and Analysis*. PhD Thesis, University of Canterbury, Christchurch.
[14] J. B. Hong and D. S. Kim. (2016). Assessing the effectiveness of moving target defenses using security models. *IEEE Trans. Dependable Secure Comput.* 13, 163–177.
[15] N. Idika and B. Bhargava. (2012). Extending attack graph-based security metrics and aggregating their application. *IEEE Trans. Dependable Secure Comput*. 9, 75–85
[16] A. Jaquith. (2007). *Replacing Fear, Uncertainty, and Doubt*. Boston, MA: Addison-Wesley.
[17] E. Jonsson and T. A. Olovsson. (1997). A quantitative model of the security intrusion process based on attacker behavior. *IEEE Trans. Softw. Eng.* 23, 235–245.
[18] A. Kott, C. Wang, and R. F. Erbacher. (2014). *Cyber Defense and Situational Awareness*. Berlin: Springer International Publishing.
[19] Leanid Krautsevich, Fabio Martinelli, and Artsiom Yautsiukhin. (2011). *Formal Analysis of Security Metrics and Risk*. Berlin: Springer.
[20] D. J. Leversage and E. J. Byres. (2008). Estimating a systems mean time to compromise. *IEEE Secur. Priv.* 6, 52–60.
[21] W. Li and R. Vaughn. (2006). "Security research involving the modeling of network exploitations graphs," in *Proceedings of Sixth IEEE International Symposium Cluster Computing and Grid Workshops*, (Rome: IEEE).
[22] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewics, M. Artz, and R. Cunningham. (2006). "Validating and restoring defense in depth using attack graphs," in *Proceedings of Military Communications Conference*, Washington, DC, 31–38.
[23] P. Mell, K. Scarforne, and S. Romanosky. *A Complete Guide to the Common Vulnerability Scoring System (CVSS)*. Available at: http://www.first.org/cvss/cvss-guide.html
[24] Nmap. (2016). *Nmap-Network Mapper.* http://nmap.org/index.html [accessed February 3, 2016].
[25] S. Noel and S. Jajodia. (2010). Measuring security risk of networks using attack graphs. *Int. J. Next Gener. Comput.* 1, 135–147.
[26] I. C. Nwokedi. (2010). *Characterizing and Aggregating Attack Graph-Based Security Metrics*. Ph.D. thesis, Purdue University, West Lafayette, IN.

[27] R. Ortalo, Y. Deswarte, and M. Kaaniche. (1999). Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Trans. Softw. Eng.* 25, 633–650.

[28] X. Ou, W. F. Boyer, and M. A. McQueen. (2006). "A scalable approach to attack graph generation," in *Proceedigs of the 13th ACM Conference on Computer and Communications Security (CCS)*, (New York, NY: ACM), 336–345.

[29] X. Ou and A. Singhal. (2011). *Quantitative Security Risk Assessment of Enterprise Networks*. New York, NY: Springer-Verlag.

[30] J. Pamula, S. Jajodia, P. Ammann, and V. Swarup. (2006). "A weakest adversary security metrics for network configuration security analysis," in *Proceedings of Second ACM Workshop Quality of Protection*, (New York, NY: ACM), 31–38.

[31] M. Pendleton, R. Garcia-Lebron, and S. Xu. (2016). A Survey on Security Metrics. *CoRR* arXiv:1601.05792v1.

[32] C. Phillips and L. P. Swiler. (1998). "A graph-based system for network vulnerability analysis," in *Proceedings of the 1998 Workshop on New Security Paradigms*, (New York, NY: ACM), 71–79.

[33] A. Roy, D. S. Kim, and K. S. Trivedi. (2012). ACT: towards unifying the constructs of attack and defense trees. *J. Secur. Commun. Netw.* 5, 929–943.

[34] A. Roy, D. S. Kim, and K. S. Trivedi. (2012). "Scalable optimal countermeasure selection using implicit enumeration on attack countermeasure trees," in *Proceeedings of the 42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, (Rome: IEEE), 1–12.

[35] K. Sallhammar, B. E. Helvik, and S. J. Knapskog. (2006). On stochastic modeling for integrated security and dependability evaluation. *J. Netw.* 1, 31–42.

[36] R. Savola. (2007). "Towards a security metrics taxonomy for the information and communication technology industry," in *Proceedings of the International Conference on Software Engineering Advances*, (Washington, DC: IEEE Computer Society), 60–60.

[37] R. M. Savola. (2007). "Towards a taxonomy for information security metrics," in *Proceedings of the 2007 ACM Workshop on Quality of Protection*, QoP '07, (New York, NY: ACM), 28–30.

[38] R. Vaughn, D. Dampier, and A. Siraj. (2002). Information security system ranking and rating. *CrossTalk J. Defense Softw. Eng.*

[39] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia. (2008). "An attack graph based probabilistic security metrics" in *Proceeedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, (Berlin: Springer), 283–296.

[40] L. Wang, A. Singhal, and S. Jajodia. (2007). "Measuring the overall network security of network configurations using attack graph," in *Proceedings of 21st Annual IFIP WG.3 Working Conference on Data and Applications Security*, Berlin.

Biographies

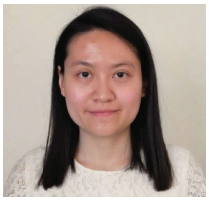


S. E. Yusuf is a staff of the Department of Computer Science, Federal University Kashere, Gombe, Nigeria. He received M.Sc. degree in Computer Science (under the supervision of Prof. Longe Olumide) from the University of Ibadan, Nigeria. He is currently a Ph.D. student at the University of Canterbury, New Zealand under the supervision of Dr. Dong Seong Kim. His research interests are in security modelling and analysis of dynamic enterprise networks and Cloud.



J. B. Hong received Ph.D. degree at the University of Canterbury, New Zealand under the supervision of Dr. Dong Seong Kim. He is a member of

the Dependability and Security (DS) Research Group (also known as the UC Cyber Security Group). His research interests are in security modelling and analysis of computer and networks, Cloud, SDN, IoT, and cyber-physical systems.



M. Ge received her M.Sc. degree in Advanced Computing – Internet Technologies with Security with Merit from the University of Bristol, UK. She is currently a Ph.D. student at the University of Canterbury, New Zealand under the supervision of Dr. Dong Seong Kim. Her research interests are security modelling and analysis of the Internet of Things, software defined networking.



D. S. Kim is the Director of the University of Canterbury Cyber Security Lab. He is a Senior Lecturer (the position is tenured and roughly equivalent to an associate professor in the North American system) in Cyber Security in the Department of Computer Science and Software Engineering at the University of Canterbury, Christchurch, New Zealand. He received Ph.D. degree in Computer Engineering from the Korea Aerospace University in February 2008. He was a visiting scholar at the University of Maryland, College Park, Maryland in the US during the year of 2007 in Prof. Virgil D. Gligor Research Group. From June 2008 to July 2011, he was a postdoc

at Duke University, Durham, North Carolina in the US in Prof. Kishor S. Trivedi. His research interests are in security and dependability for systems and networks; in particular, Intrusion Detection using Data Mining Techniques, Security and Survivability for Wireless Ad Hoc and Sensor Networks and Internet of Things, Availability and Security modelling and analysis of Cloud computing, and Reliability and Resilience modelling and analysis of Smart Grid.