Adding Network Exposure to Environmental Measures in Security Risk Scoring Models

Eli Weintraub, Yuval Cohen Afeka Tel Aviv

School of Industrial Engineering and Management

eliew@afeka.ac.ill , yuvalC@afeka.ac.il

Abstract

Hackers attack organizations on a regular basis. Managers are using vulnerability measures to evaluate the risks of the attacks they are exposed to. Information security methodologies define three major security objectives: confidentiality, integrity and availability. This work is focused on adding network exposure measures impacting on availability. The proposed approach develops measures to assess the damage for the whole network, and a set of measures to assess the risk for the single node. In terms of the single node three different risks are being measured: urgent risk, secondary risk, and disconnection risk. According to existing security assessment models, network exposure measures are either missing or considered implicitly through assessment of availability measure. In this work quantitative explicit measures for network exposure are defined, based on the organizational specific configuration, thus improving accuracy of security risk measures.

Introduction

Various kinds of damages are caused by anonymous hostiles, from stealing data, changing their software or paralyzing their website (Mell et. al, 2015). Organizations' computers are exposed to attacks for long periods of time, sometimes for weeks, from the moment a vulnerability has been detected until the time a patch is prepared. According to (Nũez, 2008) there is a need for a solution that can rapidly evaluate system damages after cyber-attacks for recovery purposes of their information system. Evaluation of potential damages is important for configuration management planning decisions. Information systems contain large amounts of software components which might contain vulnerabilities stemming from logical planning or programming bugs. Attackers plan their attacks on components having specific vulnerabilities using exploits. Organizations are exposed to damages of three kinds named CIA triads: Loss of Confidentiality, Integrity and Availability. Organizations wishing to defend their network should have accurate knowledge of its network, focusing on systems' vulnerabilities. This article focuses on using accurate knowledge of computers' components, thus enabling organizations to perform defense activities. Organizations decide on defense activities they should perform according to the amount of potential damage and according to vulnerability characteristics (Tom and Berret, 2008). When an organization is attacked, evaluating the damages the organization suffered is important for further activities needed to recover operations. Damage evaluation can be done in two ways. First, finding out the specific damages caused by the attack, which might be complicated sometimes even impossible to perform due to trace destroyed by the attacker. Second, indirectly by comparing after-attack systems' defense strength to before-attack defense strength. This work uses the second way. Risk is defined in literature as "An event where the outcome is uncertain" (Terje and Ortwin, 2009). The purpose of this research is lessening the uncertainty by proposing quantitative metrics instead of qualitative assessment to risk.

There are several definitions for availability. We use the definition of Khazanchi and Martin, (2008): Availability is the capability of an information system to make information available including all the logical and physical resources and accessible wherever and whenever they are needed, mostly evaluated using the MTBF and MTTF measures. Unavailability is defined as the complement of the availability metric to 1. Unavailability is used to measure the percentage of components that could be impacted by an attack on systems' vulnerable components. The greater the proportion of vulnerable components, the higher the score. This work proposes a new measure we name 'network exposure', which have not been considered in current scoring models. Network Exposure are the structure and characteristics of the

software/hardware components of the network including their interrelationships, which contribute to achieving good / bad availability, for example a network containing many vulnerable software components is exposed to external attackers exploiting the vulnerable components. Literature does not define any specific measure, nor scale for calculating the exposure of systems' network configuration to attacks. The proposed measure is based on the real-time information of systems' configuration, as proposed by (Weintraub(a), 2016).

Organizations use software security tools to defend themselves from cyber-attacks. Antivirus software, antispyware and firewalls are few of these tools based on periodic assessment of the target computer. Continuous Monitoring Systems (CMS) which monitor computer systems in real time are aimed at detecting vulnerabilities and notifying security managers as early as possible to limit their exposure to attackers. Contemporary systems use vulnerabilities databases which are continually updated as new vulnerabilities are detected, and make use of a scoring algorithm which assesses potential business risks.

This work focuses on measuring the network exposure by defining a formula which enable quantifying the impacts of network configuration on the exposure of the system to attacks. According to the proposed model each time a new vulnerability was published or when its status is updated, the metric is being calculated and risk scores are evaluated. Developing new accurate assessments of risk scores is critical for planning organizations' risk management activities. Using risk scores based on qualitative estimates which are currently been used, might cause organizations reaching under-mitigation situations of major risks or overmitigation situations in cases of minor risks. By using quantitative accurate risk measures, organizations will be able to build IT configurations in proportion to risk measures. The secure management of information under the conditions of frequent changes is a complex recognized problem, but the common solution is still absent (Carpenter, 2006), thus solutions like CMS's which operate continuously are necessary.

This work defines new formulas for measuring network exposure to attacks. The formula is based on three grounds: First, knowledge concerning the specifications of the attacked component within the actual configuration of the system. Second, the published history of actual cyber-attacks on the same vulnerable component. Third, the metric is a quantitative rather than qualitative measures.

The rest of the paper is organized as follows: Section 2 describes current known existing solutions. Section 3 describes access control systems. Section 4 presents the proposed framework. Section 5 presents the network exposure formulas and an illustration. Section 6 concludes and suggests future research directions.

Existing Solutions

External vulnerabilities databases are used by security risk scoring systems for evaluation of the risks organizations are facing. There are several owners of vulnerability databases (Nũez. 2008); Two popular systems are the Sans Internet Storm Center services and The National Vulnerability Database (NVD). Risk scoring systems make use of various parameters for estimating vulnerabilities' impacts on the target organization. Risk scores are evaluated through running a scoring algorithm while using the parameters for predicting potential attacks' damages. The Common Vulnerability Scoring System (CVSS) enables characterizing vulnerabilities and predicting risks by IT risk management professionals and researchers (Mell et.al, 2015).

CVSS uses three groups of parameters: basic, temporal and environmental. Each group is represented by score compound parameters used for scoring computations. Basic parameters represent the intrinsic characteristics of the vulnerability such as Attack Vector, Attack Complexity, Scope, Confidentiality, Integrity and Availability. Temporal parameters represent the vulnerabilities' specifications that might change over time due to defense activities taken such as published patches, Exploit code maturity and Remediation level. Environmental parameters represent the characteristics of vulnerabilities as configured by the specific organization, considering potential damages to that organization when exploits are being used by attackers. Basic and temporal parameters are specified by products' vendors who have the best knowledge of their product. Environmental parameters are specified by the users who have the best knowledge of their environments and attacks' impacts on their organization. For availability impact evaluation, CVSS uses three parameters: two base parameters 'scope' and 'Availability Impact', and one environmental parameter 'Availability Requirements'. Scope refers to the ability for a vulnerability in one

component to impact resources beyond its privileges, assigned values 'unchanged' or 'changed'. Availability Impact parameter measures the impact to the availability of the impacted component resulting from a successfully exploited vulnerability. Availability Requirement environmental parameter is assigned values 'high', 'medium' or 'low'. Environmental parameters include three groups of parameters indicating security importance measures in the organization: 'Confidentiality requirement', 'integrity requirements' and 'availability requirements'. 'Availability Requirement' represents the damage to the availability of the system in case of a successful attack on a component. Thus, no environmental parameter exists for measuring networks' exposure – which is the focus of this work. The environmental group of parameters enables to customize the CVSS score depending on the importance of the impacted IT asset to a user's organization. The full effect on the overall risk score is determined by the scoring algorithm by incorporating the base impact metrics into the environmental metrics producing the overall security risk score. This work suggests adding the new environmental exposure impact measure into the computations of the availability measure. The availability measure is used for overall risk scoring computations.

All CVSS parameters are assigned ordinal qualitative values which are based on the knowledge of human experts. For example the 'availability requirement' parameter is assigned values H,M,L which do not differentiate between 0.99 availability and 0.999 availability, both are considered high. Also, organizations might assign a specific availability measure as high while other organizations might assign the same availability to medium. Parameter values are not based on the specific characteristics of the network. The new suggested exposure measure will be quantitative, in contrast to current metrics.

According to (Qadir and Quadri, 2016) unavailability is not an option in todays' echo systems, given the heavy dependence of modern organizations on information resources. Availability is the least discussed and researched security attribute, although it is not the least important attribute. In fact, it plays an important role in determining the other attributes of security (confidentiality and integrity). According to (Khazananchi and Martin, 2008) availability measurements should take into consideration the logical and physical resources in order to enable accessibility whenever the information is needed. Qadir and Quadri (2016) describe the factors availability is dependent upon as software, hardware and network. Software can be further divided to three levels: service level, component level and class/object level. Since there exists a dependency and association between all these layers, it is important if there exists a bad design or logical errors in the design at the lowest level. A system might be exploited step by step by gaining access from the upper layers. Current models do not take into consideration those issues. The proposed model measures network exposure to the actual known vulnerabilities. The model considers networks' components exposure specifically, and evaluates network' exposure by considering components' interrelationships.

According to Federal Information Processing Standards (FIPS) 199.5 (Dempsey et.al., 2011), organizations assign their IT resources importance measures based on component location, business function using it, and potential losses in case the component is damaged. For example, U.S. government assigns every IT asset to a group of assets called a system. Every system must be assigned three "potential impact" ratings according to three security objectives to represent the potential impact on the organization in case the system is compromised. Thus, every IT asset in the U.S. government has a potential impact rating with respect to security objectives. CVSS follows this general model, but does not require organizations to use specific tools for assigning the impact ratings. Sandhu et. al., (1999) state that organizations should define the specifications of security risks of their specific environment. The Department of State has implemented a scoring program called iPost that is intended to provide continuous monitoring capabilities of information security risks for IT infrastructure. According to (Keller and Subramanianm, 2009) the iPOST scoring model does not define the base scores of CVSS to reflect the characteristics of its specific environment. This work presents a model aimed to close this gap.

Quantification of the environmental parameters in CVSS algorithm has been recently presented in a research demonstrating improvements in accuracy of risk scores by using the actual IT configuration (Weintraub (b), 2016). Quantifying risks based on a configuration management database system which makes use of systems' elementary components such as data tables, data items and security specifications (ibid). This paper continues the same line of research, aimed at improving risk scoring accuracy by adding a quantitative metric and basing evaluations on the specific organizations' configuration.

Access Control

Access Control refers to control how Information Technology resources are accessed so that they are protected from unauthorized modifications or disclosure (Harris, 2013). Access controls give organizations the ability to control, restrict, monitor and protect organizations' availability, integrity and confidentiality. A decision weather a user may access a specific resource is a process comprising two steps: authentication and authorization. Authentication is a process of decision if the user is who he claims to be, and authorization is a process of decision weather he is authorized access to particular resources and what actions he is permitted to perform on the resource. Authorization is a core component of every operating system, using access criteria rules to enable its decisions. Access tables manage the information weather a user has the permissions to perform varied operations on resources. Granting access rights to users should be based on the level of trust an organization has on a user and the users' need-to-know. Different access criteria can be enforced by roles, groups, location, time, and transaction type. Roles are based on organizational job assignments. Groups are a way of assigning access control rights. A group represents a couple of users who require the same types of access to information. Using groups is easier to manage then assigning rights and permissions to each user. The need-to-know principle is based on the concept that users should be given access only to the information they require to perform their duties. Giving any more rights to a user raises the possibility of that user to abuse the permissions assigned to him, thus raising the risks of illegal usage. An Access Control Model is a framework that dictates how users access resources using mechanisms to enforce the rules of the model. There are three main access control models: Discretionary Access Control (DAC), Mandatory Access Control (MAC), and Role-Based Access Control (RBAC). According to (Harris, 2013) the role based model has become predominant for advanced access control organizational needs. Access control systems enable organizations to detect illegal access to their IT systems weather by external hostiles or inner unauthorized humans.

The framework proposed by this research suggests adding new measures, enabling quantification of systems' exposure, illustrated by a case study.

The Proposed Framework

The proposed framework includes two capabilities not found in current practices (see Fig. 1). First, the environmental parameters are assigned values based on the real systems' configuration as updated in the Configuration Management Data Base (CMDB) (Keller and Subramanianm, 2009). This follows researchers stating that it is impossible for organizations to make precise estimates of the economic damages without having full knowledge of users' IT environment (Weintraub (b), 2016) (Grimalia et.al., 2009). Second, the proposed model is based on a CMS system which operates continuously and alerts of threats in real time. This follows researchers (Kotenko and Chechulin, 2014) (Khazananchi and Martin, 2008) stating that network should be monitored on a continuous basis, and vulnerabilities must be analyzed to provide management the necessary appropriate threat alerts.

In the proposed framework an examination of the published vulnerabilities is conducted, comparing real time computers' assets for existing exposures, calculating the target distribution impacts on the overall risk score. The proposed architecture and components follows:

Continuous Monitoring System (CMS).

The system runs continuously computing risk scores. Computations of distribution impact scores are performed in three cases:

1. In case a new published vulnerability or status changed in NVD.
2. In case a configuration change is made to the systems.
3. In case the access control system signals that a certain systems' component was exploited by a cyber-attack or an un-authorized user.

Vulnerabilities database (NVD).

Vulnerabilities database includes all known vulnerabilities as published by database owners. Examples of vulnerability specifications used by NVD are: vulnerability category, vendor name, product name, published vulnerability start and end dates, vulnerability update dates, vulnerability severity, access vector, and access complexity (Dempsey et. al., 2011).

The Common Vulnerability Scoring system (CVSS).

The risk scoring system is the algorithm this research uses for illustration of the proposed model. CVSS computes security risk scores using a set parameter groups: basic, temporal and environmental.

Configuration Management Database (CMDB).

CMDB is a database which includes metadata on all hardware and software components of the target system including the specifications of each component such as hardware/software type, model, version, amount of internal memory, external storage. CMDB includes also the calculated risk scores of each component. Risk scores are recalculated each activation of the CMS system.

Access Control System.

The module controls and monitors all target systems' components. When the module recognizes an illegal access or an attack on a certain component it alerts operators and interrupts or terminates processes. Illegal access to systems' components may be caused by hackers, illegal user or software flaws. Hostiles look for vulnerabilities or backdoors which let them bypass the access control system or change systems' logic, thus reaching illegally data or software components.

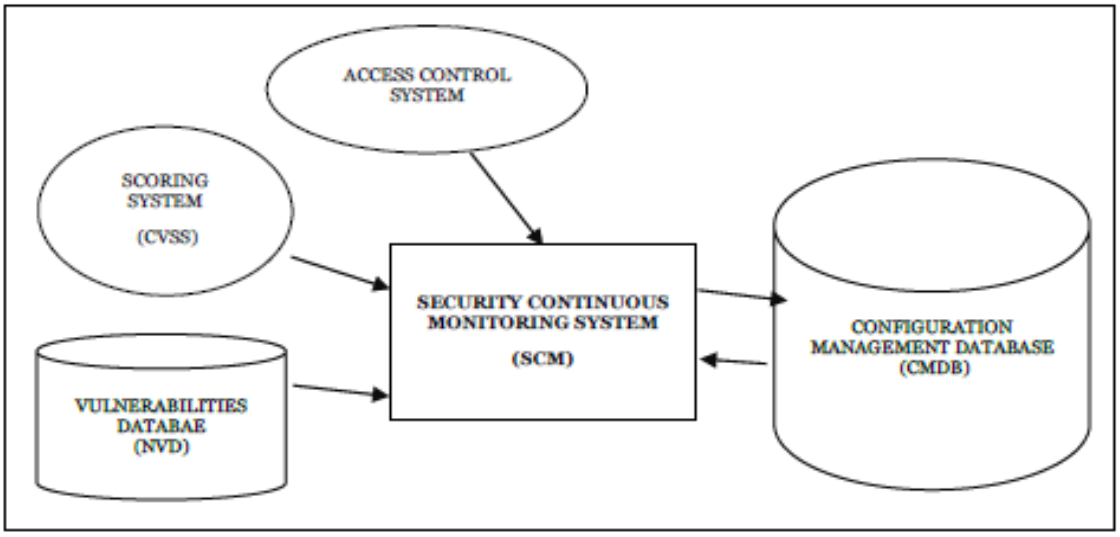

Figure. 1. Security Continuous Monitoring System framework - SCMS

Network Exposure Formulas and Computations

The proposed approach gives estimates to the risk of losing availability meaning the risk of system malfunction or system failure. It gives both overall network measures, as well as risk measures for single nodes.

In case, where the organizational network is attacked the following three measures are suggested.

1) **Damage%:** Percentage of nodes impacted : range of values is [0 to 1].

2) **Dispersion:** The ratio d/D' between d=maximal diameter of the impacted nodes, and *D*'=maximal total network diameter: **range of values is [0 to 1].**
   Where **D** the number of links in the maximal shortest path that connects between each pair of nodes; and **d** is the number of links in the maximal shortest path that connects between each pair of un-impacted neighbors of the impacted nodes.
3) **Concentration:** The ratio of m/M between m= number of impacted nodes with atleast 2 neighboring impacted nodes, and M=total number of impacted nodes. **Range of values is [0 to 1].**

In case where the organization is a node in the larger network, and in cases of measuring the exposure of a specific node in an organizational network, the following three measures are proposed:

1) **Directs:** defined as ***Dir/D***; where ***D*** is the node degree (number of arcs emanating from it), and ***Dir*** is the number of impacted direct links: range of values is [0 to 1] .
2) **Seconds:** defined as ***Sec/D*** where ***D*** is the node degree (number of arcs emanating from it), and ***Sec*** is the number of links to working nodes having direct links to impacted node. The Seconds range of values is [0 to 1].
3) **Disconnection risk**: defined as (1/***W*****),** where ***W*** is the number of arcs connected to working nodes (with the exception that when this number is zero (disconnection), *W*=1). Thus, when only one arc is connected to a working node *Disconnection risk* =1; and when all arcs are connected to working nodes, the *Disconnection risk* =1/*D* (where ***D*** is the node degree).

Illustartion: Example

The following case study illustrates the suggested measures, their computations, their meaning and effectiveness and their importance. Figure 2 describes an example network with 20 computerized nodes after a first wave of attacks which culminated with failures of nodes 14, 16, and 17.

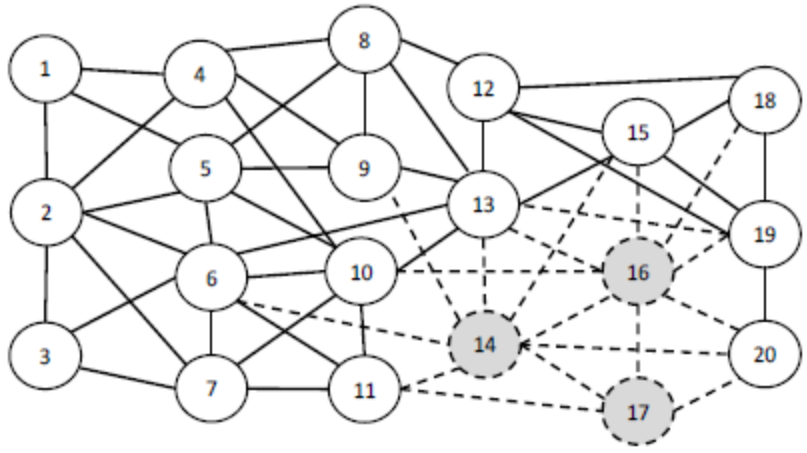

Figure. 2. The 20 computer nodes network example with 3 impacted nodes (denoted by grey and dashed lines) and dashed lines are disconnected communication lines due to the hackers attack.

In Figure. 2 the network exposure measures are:

1) **Damage %:** percentage of nodes impacted: 3/20= 0.15.
2) **Dispersion**: The ratio *d/D'* =3/5 = 0.6. Where ***d*** the diameter of the impacted nodes: **3**, and ***D'*** the network diameter is ***5***.
3) **Concentration**: The ratio of *m/M* = 3/3 = 1 the number of impacted nodes: **3** each is connected to the other two.

To illustrate the node measures for fig. 2, we chose to compute measures for nodes: 20, 15, 9, 6, 3. For brevity purpose we shall use: "Directs" for directly impacted neighbors, "Seconds" for second degree impacted neighbors, and "Arcs" for the degree of the non-impacted node.

For node 20: *Directs* = 3/4, *Seconds* = 1/4 (node 19 "Directs">0), *Disconnection risk* =1/1=1

For node **15**: *Directs* = 2/6, *Seconds* = 3/6 (13, 18, 19 have "Directs">0), *Disconnection risk* =1/4

For node **9**: *Directs* = 1/5, *Seconds* = 1/5 (node 13 have "Directs">0), *Disconnection risk* =1/4

For node **6**: *Directs* = 1/8, *Seconds* = 3/8 (10, 11, 13 have "Directs">0), *Disconnection risk* =1/7

For node **3**: *Directs* =0, *Seconds* = 0, *Disconnection risk* =1/3

It follows that immediate risk is highest for node 20 with ***Directs*=3/4** (followed by node 15), while risk evolution potential is highest for nodes 15 and 6 with ***Seconds*=3/6 and 3/8**, respectively, and disconnection risk is highest for node 20 (*Disconnection risk* **=1**).

The example follows with hacker attack evolution as depicted in Figure 3.

Figure 3 illustrates the example network with 20 computerized nodes after a second wave of attacks which culminated with failures of nodes 9, 13, 19 (in addition to previously failed nodes: 14, 16, and 17).

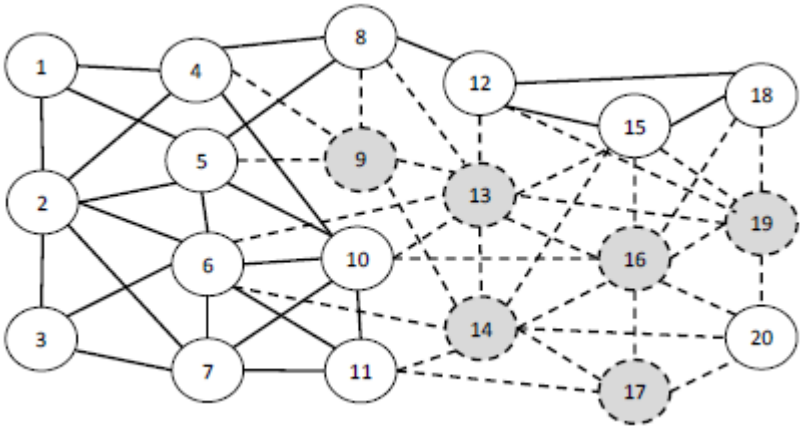

Figure 3. The 20 computer nodes network example with 6 impacted nodes (denoted by grey and dashed lines - dashed lines are disconnected communication lines due to the hackers' attack.)

In Figure 3 the network exposure measures are:

1) **Damage %**: **6/20= 0.3** twice the number in Fig. **2**
2) **Dispersion**, the diameter of the impacted nodes: **4/5** (the number of links in the maximal path that connects minimally between each pair of un-impacted neighbors of the impacted nodes) for example: 20-16-13-9-4. Diameter of 4 is an increase from 3 in fig. 2.
3) **Concentration:** The largest connected group of at least two neighboring impacted nodes = **6** which is as large as the number of impacted nodes=6. So: 6/6=1.

To illustrate the node measures for fig. 3, we compute measures for nodes: 20, 15, 9, 6, 3. These could be easily compared to the measures for Fig. 2.

For node 20: *Directs* = 4/4, *Seconds* = 0, *Disconnection risk* =1 (disconnected)

For node **15**: *Directs* = 4/6, *Seconds* = 2/6 (12, 18 have "Directs">0), *Disconnection risk* =1/2

For node **9**: Impacted.

For node **6**: *Directs* = 2/8, *Seconds* = 3/8 (5, 10, 11, have "Directs">0), *Disconnection risk* =1/6

For node **3**: *Directs* =0, *Seconds* = 1/3 (node 6 have "Directs">0), *Disconnection risk* =1/3

Thus, node 9 failed, node 20 is disconnected (*Disconnection risk* =1), node 15 faces high immediate and intermediate risk along with disconnection risk. Node 6 has immediate and intermediate risk exposure, but its disconnection is unlikely (*Disconnection risk* =6). Finally, node 3 has small intermediate risk exposure (Seconds=1).

These measures help the decision makers in prevention actions. For example, node 20 would be very interested in adding a link to node 15, or 12. Moreover, to decide on restoration priorities, the impact of restoring alternative nodes could be simulated. For example, suppose that the resources for restoration are limited to one node at a time. Comparing alternatives would be an efficient decision support tool. For example, in figure 2: comparing restoration of node 16 to node 17 yields the following measures.

Referring to figure 3, a single restoration would change the number of impacted nodes from 6 to 5 and the impact on network measures are relatively small:

<u>For restoring node 16 – network measures:</u> Damage % =5/20; Dispersion=4/5; **Concentration=4/6**

<u>For restoring node 17– network measures:</u> Damage %=5/20; Dispersion=4/5; **Concentration=5/6**

The impact of restoration is always on specific neighboring nodes. So for restoring node 16 vs. 17: the neighboring node of 16 and 17 are nodes 20 and 15. The measures for node 20 are the same, but for node 15 the measures slightly in favor of 16.

For node 20: *Directs* = 3/4, vs. 3/4, *Seconds* = 1 vs. 1, *Disconnection risk* =1 vs. 1

For node 15: *Directs* = 3/6, vs. 4/6, *Seconds* = 3/6 vs 2/6 (12, 18 have "Directs">0), *Disconnection risk* =1/3 vs. 1/2

Thus, restoring node 16 (vs. restoring node 17) has smaller direct risk, higher secondary risk, but more arcs=less disconnection risk.

Thus, it may be concluded that restoring node 16 has a priority over node 17.

Conclusions

This work presents a new framework of a Security Continuous Monitoring System, structure and mechanisms. The CMS uses CVSS scoring model for risk scoring, operating in real time. According to the proposed model CVSS will use new network exposure environmental parameters which are evaluated using a new formula based on the configuration of the system. The new measures are quantitative, normalized to [0..1] and based on the actual configuration. This is contrary to existing model which do not measure the impacts of network exposure on the overall risk, at most consider network configuration implicitly relying on intuitive managers' assessment.

The model helps risk managers in assessing the damage to attacks on firms' components after a cyber-attack. Using the proposed model will bring more accurate estimates to network configuration risks, thus enabling efficient risk mitigation plans and improved defense to organizations.

Network exposure metrics enable to customize the CVSS score depending on the importance of the impacted IT asset to a user's organization. According to the proposed model, a formula which assigns quantitative measures to exposures' impacts based on the actual impacts of an attack on the specific component. The proposed model outlines the structure of a CMS which uses the real organizational

environment and components, and the processes which update the network exposure parameters with the planned and actual values. The framework enables getting accurate measures, thus enabling the organization making better risk management decisions, allocating risk management budgets in proportion to the risks.

Future improvements may focus on building a full dash-board of system exposure metrics from its component measures.

More research is needed in studying the impacts of the various proposed network exposure measures on the overall security risk score.

References

Carpenter , B. (2006). The Internet Engineering Task Force. Overview, Activities, Priorities. *IETF Report to ISOC BoT, Oct. 2006.*

Dempsey, K. & Chawia, N.S. & Johnson. A. & Johnson.R. & Jones. A.C. & Orebaugh. A. & Scholl. M. & Stine. K. (2011). Information security continuous monitoring (ISCM) for federal information systems and organizations. *NIST.*

Grimalia. M.R. & Fortson L. W. & Sutton. J. L. (2009). Design considerations for a cyber incident mission impact assessment process. *Proceedings of the Intrnational Conference on Security and Management (SAM09), Las Vegas.*

Harris. S. (2013). All in one CISSP Exam Guide. 6Th Ed. *McGraw Hill Education.*

Keller. A. & Subramanianm. S. (2009). Best practices for deploying a CMDB in large-scale environments. *Proceedings of the IFIP/IEEE International conference and Symposium on Integrated Network Management, pages 732-745, NJ, IEEE Press Piscataway.*

Khazanchi. D. & Martin. A. P. (2008). *Information Availability: Handbook of Research on Information Security and Assurance.*

Kotenko. I. & Chechulin. A. (2014). Fast network attack modeling and security evaluation based on attack graphs. *Journal of Cyber Security and Mobility Vol. 3 No. 1 pp 27-46.*

Mell. P. & Scarfone. K. & Romanosky. S. (2015). CVSS – Common Vulnerability Scoring System v3.0: Specification Document. *FIRST Org.*

Nũez. Y. F. (2008). Maximizing an organizations' security posture by distributedly assessing and remeding system vulnerabilities. *IEEE – International Conference on Networking, Sensing and Control, China, April 6-8, 2008.*

Qadir. S. & Quadri. S.M.K. (2016). Information Availability: An insight into the most important Attributes of Information security. *Journal of Information Security, 2016, 7, 185-195.*

Sandhu. R. & Ferraiolo. D. & Kuhn. R. (1999). The NIST Model for Role-Based Access Control: Towards A Unified Standard. *George Mason Univ.*

Terje. A. & Ortwin. R. (2009). On risk defined as an event where the outcome is uncertain. *Journal of Risk Research Vol. 12.*

Tom. S. & Berrett. D. (2008). Recommended practice for patch management of control systems. *DHS National Cyber Security Division Control Systems Security Program.*

Weintraub. E. (a). (2016). Security Risk Scoring Incorporating Computers' Environment. (IJACSA) *International Journal of Advanced Computer Science and Applications, Vol. 7(4), April 2016.*

Weintraub. E. (b). (2016). Evaluating Damage Potential in Security Risk Scoring Models. *International Journal of Advanced Computer Science and Applications (IJACSA), 7(5), 2016.*