Evaluating Confidentiality Impact in Security Risk Scoring Models

Eli Weintraub
Department of Industrial Engineering and Management
Afeka Tel Aviv Academic College of Engineering
Tel Aviv, Israel

***Abstract*—Risk scoring models assume that confidentiality evaluation is based on user estimations. Confidentiality evaluation incorporates the impacts of various factors including systems' technical configuration, on the processes relating to users' confidentiality. The assumption underlying this research is that system users are not capable of estimating systems' confidentiality since they lack the knowledge on the technical structure. According to the proposed model, systems' confidentiality is calculated using technical information of systems' components. The proposed model evaluates confidentiality based on quantitative metrics rather than qualitative estimates which are currently being used. Frameworks' presentation includes system design, an algorithm calculating confidentiality measures and an illustration of risk scoring computations.**

Keywords—information security; risk management; continuous monitoring; vulnerability; confidentiality; risk assessment; access control; authorization system

I. INTRODUCTION

Cyber-attackers cause damage to organizations and personal computers by stealing their business or private data and by making changes in their software and hardware [1]. The damages are usually categorized by security experts to three kinds: loss of confidentiality, integrity or availability. Vulnerabilities are software weaknesses or exposures. An attack is performed by exploiting software vulnerabilities in the target system. Attackers make use of vulnerabilities stemming from bugs that are potential causes to security failures. Exploits are planned to attack certain components having specific vulnerabilities. Users' computers might be damaged by exploited vulnerabilities. Defending computers depends on the amount of knowledge an organization has of their computing systems' vulnerabilities. This work focuses on gaining accurate knowledge of computers' configuration, thus enabling improved risk mitigation to defend computers from threats caused by attackers. Accurate knowledge of computers' risks assist security managers to adopt security measures effectively. Reference [2] states that Stuxnet worm included a process of checking hardware models and configuration details before launching an attack. Risk managers make decisions on activities actions they have to perform in order to limit their exposure to risks according to the amount of potential damage and vulnerability characteristics [3].

Risk has many definitions in research publications. This research uses the definition of [4]: "An event where the outcome is uncertain". Accordingly, this work is aimed at lessening risk uncertainty. The proposed model focuses on an improved confidentiality impact assessment algorithm which is based on the real-time information on systems configuration, as proposed by [5].

Several software products are used to defend computers from cyber-attackers. Antivirus software, antispyware and firewalls are examples to some of these tools based on periodic assessment of the target computer by comparing computers' software to the known published vulnerabilities. Continuous Monitoring Systems (CMS) monitor systems in a near real time process aimed at detecting vulnerabilities and notifying security managers. Contemporary systems use vulnerabilities databases which are continually updated as new vulnerabilities are detected and a scoring algorithm which predicts potential business damages. This work focuses on measuring the confidentiality impacts on the overall risk score. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to unauthorized ones. Evaluating confidentiality impacts on business risk will be based on an algorithm which compares the actual access users are gaining, to the rules defined by the authorization system. The proposed CMS evaluates business risk scores relating to the actual technical configuration. This model focuses on measuring confidentiality potential losses related to known vulnerabilities. According to the proposed model each time a system is breached, systems' risk score is re-evaluated to reflect the impacts of the new breach.

Computers are at risk to known threats until the time a patch is prepared for defending the vulnerable software, an activity that may last weeks or months. In today's environment of zero-day exploits, conventional systems updating for security mitigation activities has become a cumbersome process. There is an urgent need for a solution that can rapidly evaluate system vulnerabilities' potential damages for immediate risk mitigation [6].

Security Continuous Monitoring (SCM) is a specific subgroup of CMSs that use techniques for monitoring, detecting and notifying of security threats. After identifying these risks, the tools evaluate the potential impacts on the organization. Reference [7] states that SCM systems are aimed at closing the gap between the zero-day of identifying the vulnerability, until the moment the computer is loaded by a patch.

This paper describes the mechanisms of a new SCM framework that will produce better risk scores than current known systems. The proposed framework defines processes on two grounds: 1) knowledge concerning real computers' configuration of the target system, and 2) an algorithm which runs continuously and computes confidentiality impact assessments.

The rest of the paper is organized as follows: In section II a description of current known security scoring solutions. In section III a description of access control systems. In section IV a presentation of the proposed framework including systems architecture. In section V a description of the confidentiality algorithm and risk scoring model. In section VI presentation of the results. In section VII conclusions and future research directions.

II. Existing Solutions

SCM systems are using external vulnerabilities databases for evaluation of the target computers' risk. There are several owners of vulnerability databases [6], for example the Sans Internet Storm Center services and The National Vulnerability Database (NVD). Vulnerability Identification Systems (VIS) aimed to identify vulnerabilities. Examples for VIS systems are The Common Vulnerabilities and Exposures (CVE), and The Common Weakness Enumeration (CWE).

This work uses NVD vulnerabilities database as an illustration of the proposed model.

Risk evaluation uses scoring systems which makes use of systems' characteristic parameters for estimating vulnerabilities' impacts on the organization. The Common Vulnerability Scoring System (CVSS) is a framework that enables user organizations benefit by receiving IT vulnerabilities characteristics [1].

CVSS uses three groups of parameters to score potential risks: basic parameters, temporal parameters and environmental parameters. Each group is represented a vector of parameters which are used to compute the score. Basic parameters represent the intrinsic specifications of the vulnerability. Temporal parameters represent the specifications of a vulnerability that might change over time due to technical changes. Environmental parameters represent the specifications of vulnerabilities derived from the local IT specific environment used by users' organization. CVSS enables omitting the environmental metrics from score calculations in cases the users do not specify the detailed description of environment and components.

CVSS is a common framework for characterizing vulnerabilities and predicting risks, used by IT risk managers, researchers and IT vendors. It uses an open framework which enables managers to deal with organizations' risks based on systems' characteristics. Organizations adopting CVSS framework may gain the following benefits:

- A standard scale for characterizing vulnerabilities and scoring risks.
- Normalizing vulnerabilities according to specific IT platforms.
- An open framework. Organizations can see the characteristics of vulnerabilities and the logical process of scoring evaluation.
- Environmental scores. Considering changes in its IT environment according to predicted risk scores.

There are few other vulnerability scoring systems besides CVSS differing by the parameters' specifications and scoring scales. CERT/CC emphasizes internet infrastructure risks. SANS vulnerability system considers users' IT configuration. Microsoft emphasizes attack vectors and vulnerabilities' impacts.

Using CVSS scoring system, basic and temporal parameters are specified and published 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 business impacts.

This paper focuses on environmental metrics.

Business damages caused by a vulnerability are influenced by the IT exploited component. CVSS environmental parameters specify the characteristics of a vulnerability that is associated with user's IT configurations' components. Environmental parameters are of three groups:

1) Collateral Damage Potential (CDP).
Measures specifying the economic potential damage caused by a vulnerability.

2) Target Distribution (TD).
The percentage of vulnerable components in users' environment.

3) Security Requirements (CR, IR, AR).
Security importance measures in users' organization. Those parameters are subdivided to parameters indicating the Confidentiality Requirement (CR), integrity (IR), and availability (AR). Higher security requirements may cause higher security damages on the organization.

Confidentiality impacts measure the impact on confidentiality of a successfully exploited vulnerability. Confidentiality refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to unauthorized ones. Confidentiality is evaluated using two parameters: Confidentiality Impact (CI) which is a basic parameter, and Confidentiality Requirement (CR) which is an environmental parameter. CI may be assigned three values: N, P, and C. Increased CI increases the vulnerability score. None (N) is defined whenever there is no impact to the confidentiality of the system. Partial (P) is whenever there is considerable informational disclosure, access to some system files is possible, but the attacker does not have control over what is obtained, or the scope of the loss is constrained. Complete (C) is defined when there is total information disclosure, resulting in all system files being revealed. CR is an environmental parameter used for different environments which may have varying impacts on the final evaluation of business risk. CR is one out of three Security Requirement parameters belonging to the environmental group.

The environmental group of metrics enables the analyst to customize the CVSS score depending on the importance of the affected IT asset to a user's organization, measured in terms of confidentiality, integrity, and availability, that is, if an IT asset supports a business function for which availability is most important, the analyst can assign a greater value to availability, relative to confidentiality and integrity. Each security requirement has three possible values: "low," "medium," or "high". The full effect on the environmental score is determined by the corresponding base impact metrics. That is, these metrics modify the environmental score by reweighting the base confidentiality, integrity, and availability impact metrics. The CI metric has increased weight if the CR is "high". The greater the security requirement, the higher the score.

CR may get four values. Low (L) for cases of loss of confidentiality which have only a limited adverse effect on the organization or individuals associated with the organization (e.g., employees, customers). Medium (M) for loss of confidentiality for cases having serious adverse effects on the organization or individuals associated with the organization. High (H) for cases of confidentiality losses which have a catastrophic adverse effect on the organization. Not Defined (ND) for situations having no environmental impact on confidentiality score.

Categorization of IT components according to security requirement measures should encompass all assets to raise the possibility of predicting organizational risks. Federal Information Processing Standards (FIPS) requirements demands implementation of a categorization [7], but does not require using any particular scale, thus risk comparison of users' systems is difficult.

III. Access Control

Access Control refers to control how Information Technology resources are accessed so that they are protected from unauthorized modifications or disclosure [8]. Access controls are security features that control how users and systems interact with other systems and resources and protect the resources from unauthorized access. Access controls give organizations the ability to control, restrict, monitor and protect resource availability, integrity and confidentiality. This paper focuses on confidentiality. Several kinds of information are more sensitive than other and require a higher level of confidentiality. Information such as health records, financial information and military plans are high confidential and need more control mechanisms and monitoring to provide confidentiality. Organizations should identify the data that must be classified to ensure that the top priority of security protects this information. On the other end organizations should allocate less budgets to protect information which is less sensitive. Organizations should define varying access controls techniques to limit access to the sensitive information in accordance to the sensitivity level of the information. Organizations should define rules that outline the sensitivity levels of the varying kinds of information, and define the identity of users which will gain legal access to each information.

A decision weather a user may access 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 whether he is authorized to access a particular source and what actions he is permitted to perform on the resource. Authorization is a core component of every operating system, but application and the resources themselves sometimes perform this functionality. Authorization processes use access criteria matrixes to provide their decisions. Access matrixes manage the information weather a user has the permissions to perform varied operations on particular 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. The different access criteria can be enforced by roles, groups, location, time, and transaction type. Roles are based on organizational functions the user may perform during his work. Group is a couple of users who require the same types of access to information and resources. Using groups is easier to manage then assigning permissions to each user. The need-to-know principle is similar to the least-privilege principle. It is based on the concept that users should be given access only to the information they require in order to perform their job duties. Giving any more rights to a user rises 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. It uses mechanisms to enforce the rules of the model.

There are three main access control models. Discretionary Access Control (DAC), Mandatory Access Control, and Role-Based Access Control (RBAC). In DAC data owners decide who has access to resources. Access Control Lists (ACL) are used to enforce access decisions. In MAC, operating systems enforce the systems' policy through security labels. In RBAC access decisions are based on each subjects' role and his hierarchical functional level. According to [9] RBAC has become the predominant model for advanced access control because it reduces development and management costs. A variety of IT vendors, including IBM, Sybase, Secure Computing, and Siemens developed products based on this model.

Once an organization determines what type of access control model it will use, it needs to decide what technique to use to support the access control model. There are several techniques: Rule-Based, Constrained User Interfaces, Matrix. Content-Dependent and Context-Dependent. Rule-Based Access Control techniques are based on specific rules that indicate what can and cannot do a user on a resource. Constrained User Interfaces restrict users' access abilities to resources. Access Control Matrix is a table of subjects and objects indicating what actions each subject can perform on a specific object. Subject may represent users or roles or groups of users, object may represent technological resources. Content-Dependent Access Control is determined by the content within the object. The content dictates which user is authorized to access the object. Context-Dependent Access Control uses collection of information residing in the environment of the subject and object.

The model presented in this paper will use a RBAC model, using an Access Control Matrix technique.

IV. The Proposed Framework

Federal organizations are moving from periodic to continuous monitoring implementing SCM's which will improve national cyber security posture [10]. The proposed framework includes two capabilities not found in current practices. First, the environmental parameters are based on the components of the system as updated in the systems' Configuration Management Data Base (CMDB) [11]. This capability enables basing the scoring models to predict organizational damages to organizations' confidentiality scores relating to actual IT configuration rather than on user's estimates as proposed by [12]. According to [13] it is impossible for organizations to make precise estimates of the economic damages caused by an attack without having full knowledge of users' IT environment. Ref. [14] [5] state that network configuration should be monitored continually and available vulnerabilities must be analyzed in order to provide the necessary security level.

The proposed Security Continuous Monitoring System (SCMS) examines a database of published asset vulnerabilities, compares in real time computers' assets for existing exposures and calculates confidentiality impact measures for business risk score computations. The SCMS proposed architecture presented in Fig. I. Following, a description of systems' structure and modules, followed by modules functionality.

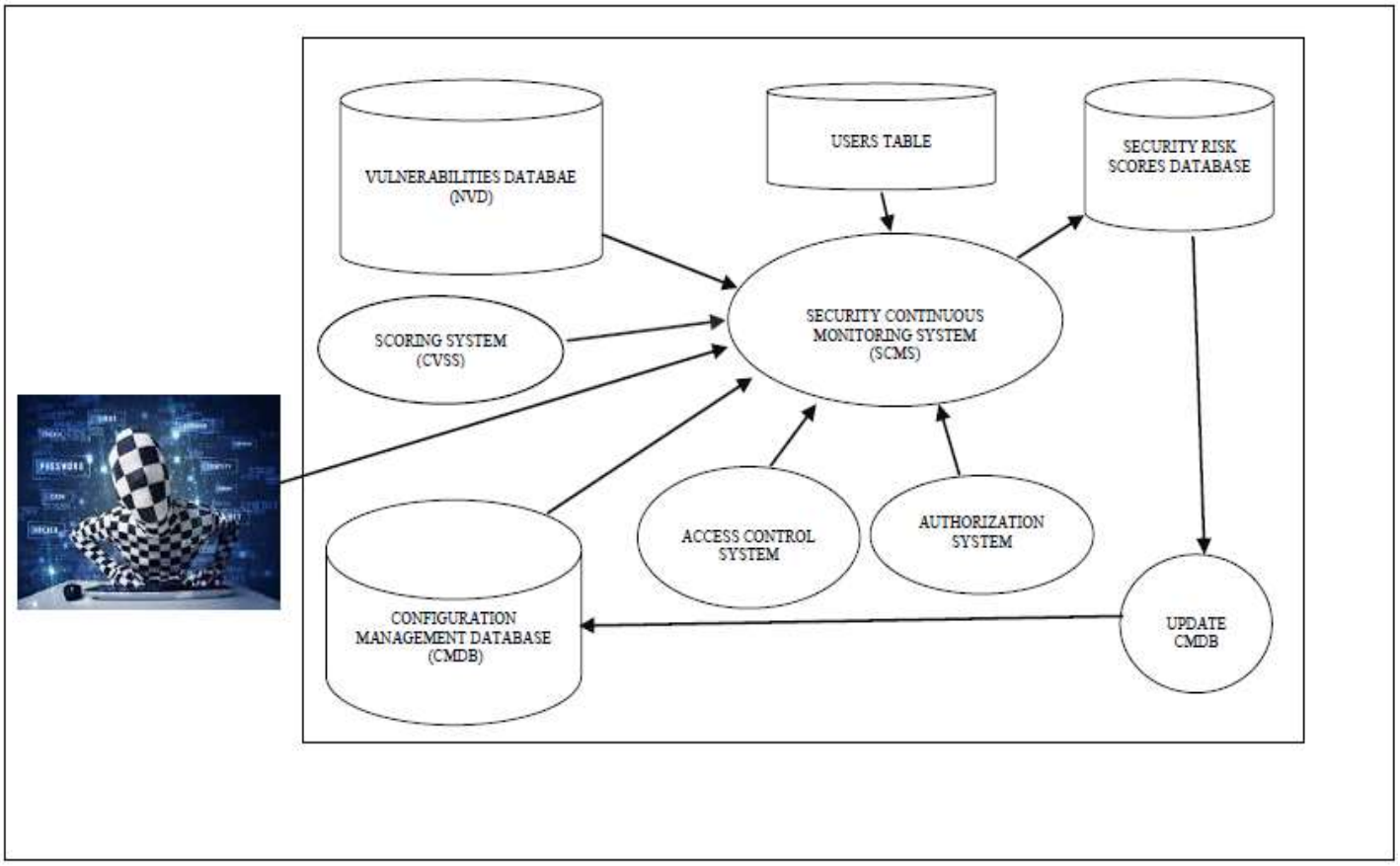

Fig. 1. Security Continuous Monitoring System architecture

- Security Continuous Monitoring System (SCMS)

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

- When a new vulnerability is published and indicated in NVD.
- When a change is made in a systems' component and indicated in CMDB.
- When the Access Control System signals that a certain component was illegally accessed or breached.

SCMS makes use of the Confidentiality Impact scoring algorithm defined in this paper.

- Vulnerabilities database (NVD).

Vulnerabilities database includes all known vulnerabilities and their specification 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 [7].

- The Common Vulnerability Scoring System (CVSS)

CVSS is the algorithm this research uses for illustration of the proposed model. CVSS computes security risk scores according to parameter groups: basic, temporal and environmental. There are also other known scoring algorithms, some of them for public use other commercial.

- Configuration Management Database (CMDB).

CMDB is a database which manages all the information of hardware and software components of the target system. The target system might be one computer or a group of organizations' network computers. According to the proposed model the CMDB includes detailed information of components' risk scores as well as detailed information of all software components. CMDB includes the information on software programs and services, and of data managed by the target system. Data is specified in the resolution of databases, tables and data items. Input/output interfaces are handled using screen-names, reports and messages. The CMDB includes information relating to risks: Security requirements (CR, IR, AR) of each component in the system. CMDB manages also the calculated CI's of systems' components. CI's are calculated using the algorithm described in this paper. CI scores are re-weighted according the environmental CR computed scores. In every activation of the SCMS system, the CI is calculated, written to the Security Risk Scores database. While calculating the CIs the CVSS module calculates the updated risk score.

- Security Risk Scores Database.

The database includes all computed risk scores and confidentiality impact scores calculated computed by SCMS. The computed scores are then updated in the CMDB by the Update CMDB module.

- Update CMDB

In cases of updates to systems' risk scores as calculated by the SCMS, CI scores and risk scores are passed to the Update CMDB module for CMDB updating. CMDB risk scores represent the updated risk scores and confidentiality impact scores for all systems' components. This update process is needed to prevent unnecessary risk scoring heavy computations which were already evaluated and has been written in the CMDB.

- Users Table

This Table includes all systems' users, weather manual or machine. Each user is identified by a User-ID. A user may include several user-roles for interfacing with the authorization system. Each user-role resembles a set of access rights to specified systems' components. For example a bank teller may have two roles which define two processes performed by him. Those processes access system components. For example, giving a loan to a customer uses a role which needs access to the loans table and customers table. Second role may be depositing cash to customers' account, which needs access to deposits table, customers table and current accounts module. In order to find out what the user is authorized to do interacting the system, one has to read all his roles in users' table, then get each user-roles' authorizations from the authorization system.

- Authorization system.

This system is responsible for management of all system applications' accesses to systems' components related to a role. Whenever an application wants to perform a users' task, it calls the authorization system by supplying the user-ID, user-role and the operation needed. The Authorization systems' reply includes an answer weather the user is authorized to perform the requested operation on the component or he is not. Operations may be read, write, update or view the component. Usually, Authorization Systems are planned as rule-base systems which uses the parameters: user-role and requested operation and other parameters such as time and place of the needed operation. Regularly, Authorization Systems manage access to database items, not to other system components such as processes, operating systems utilities, and hardware devices. Such other components are regularly managed by an Access Control System.

- Access Control System

This system controls and monitors all computers' components: hardware, software, databases, communication, system software and utilities. When the system recognizes an illegal access to a certain component it alerts operators and according to rules, interrupts or terminates processes. Illegal access to systems' components may be caused by hackers or software bugs. Hackers look for vulnerabilities or backdoors which let them bypass the authorization system rules, thus reaching illegally data or software components. In such cases it will notice the SCMS about illegal users for dropping down their authorizations and computing the new components' risk score.

V. THE RISK SCORING ALGORITHM

CVSS's framework is based on three kinds of parameters: basic, temporal and environmental parameters. According to [7], in many organizations IT resources are labeled with criticality ratings based on network location, business function, and potential losses. For example, the U.S. government assigns every unclassified IT asset to a grouping of assets called a system. Every system must be assigned three "potential impact" ratings to show the potential impact on the organization if the system is compromised according to three security objectives: Confidentiality, Integrity, and Availability. Thus, every unclassified IT asset in the U.S. government has a potential impact rating of low, moderate, or high with respect to the security objectives of confidentiality, integrity, and availability. This rating system is described within Federal Information Processing Standards (FIPS) 199.5 [15]. CVSS follows this general model of FIPS 199, but does not require organizations to use any particular system for assigning the low, medium, and high security impact ratings. References [15] [16] state that organizations should define security risk specifications of their environment, but does not define the ways organizations have to specify that information. The Department of State has implemented an application called iPost and a risk scoring program that is intended to provide continuous monitoring capabilities of information security risk to elements of its information technology infrastructure. According to [17] the iPOST scoring model does not refine the base scores of CVSS to reflect the unique characteristics of its environment. Instead, it applied a mathematical formula to the base scores to provide greater separation between the scores for higher-risk vulnerabilities and the scores for lower-risk vulnerabilities. This technique provides ordinal qualitative scores but not real quantitative measures. This work is targeted to fill-in this vacuum.

The CMDB defined in this work presented in Table I, handles configurations' information of the target system including the following entities: database tables, software components, system components such as operating system, database management systems, utility programs, development components, UI screens, etc. Each component is describes including knowledge relating to security requirements needed for operation of the risk scoring algorithm. The CMDB manages five kinds of environmental information for every system component. Table I includes information concerning the characteristics assigned to systems' components. Characteristic values are based on [15] definitions. The information is categorized according to its security type which is defined as a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management). Reference [15] states that the potential impact is low if the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals. The potential impact is moderate if the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals. The potential impact is high if the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

TABLE I. CMDB – COMPONENTS TABLE

Column ID	Column Name	Column Description	Values (*)
COMPONENT ID	Software or Hardware, Vendor, Serial No', Version…	Value is equal to component ID in NVD	unique
COMPONENT TYPE	Hardware Type (cpu, printer, disk…), Software type, etc'	For example: Database, Table, Column….	H, S, UI, COMM …
CONFIDENTIALITY IMPACT (CI)	Basic parameter	None, Partial, Complete	N, P, C
CR	Confidentiality Requirement	The importance of the affected IT asset to a user's organization, measured in terms of confidentiality.	L,M,H
IR	Integrity Requirement	Guarding against improper information modification or destruction.	L,M,H
AR	Availability Requirement	"Ensuring timely and reliable access to and use of information…".	L,M,H
FINAL EVALUATED RISK SCORE	CVSS final Risk Score based on all basic, temporal and env' parameters.	Based on all parameters including CI and CR.	0-10

(*) N=none, L=low, LM=low medium, M=medium, MH=medium high, H=high

- Confidentiality Scoring

Confidentiality of a component refers to limiting information access and disclosure to only authorized users, as well as preventing access by, or disclosure to, unauthorized ones. CVSS model uses the CR environmental parameter which is assigned three values: Low, Medium and High. According to the proposed model, suggested by [18] CR will get quantitative values on the scale [0, 1] assigning real values instead of three qualitative ordinal values H, M, and L. A new algorithm will compute the CR values according to the following formula (1):

$$(1) \qquad \mathrm{CR}(c) = \frac{\mathrm{LegalLost}(c)}{2 * \mathrm{LegalNorm}(c)} + \frac{\mathrm{ILegalPermited}(c)}{2 * \mathrm{ILegalNorm}(c)}$$

LegalLost = Legal users who lost their permissions.
LegalNorm = Number of users authorized according to the Authorization system to perform operations on component c.

IlegalPermitted = Ilegal users who actually got permissions.
IlegalNorm = Users who normally have no legal access.

CR is computed by summing the quotient of users who lost their permissions out of all legal authorized users, added to the quotient of illegal users who got permissions out of all illegal users, according to the authorizations' norm.

0 <= CR <= 1

Following the pseudo code for parameter calculations:

LegalNorm (c) = Count number of users authorized to access component c, over all their roles for each role having at least one legal authorization to c.

ILegalNorm (c) = Count number of users authorized to access component c, over all their roles for each role having no legal authorization to c.

LegalLost (c) = Count number of users authorized to access component c who have NO ACTUAL access to c and have at least one DEFINED legal authorization to c.

ILegalPermitted (c) = Count number of users who have ACTUAL access to c and are not defined as legal authorizations for c.

To illustrate the rational of the formula we assume an application planned for 10 workers, among them 3 legal authorized users and 7 illegal users, which use other applications. The illustration includes five cases of CR computations.

Implementation of the formula involves performing an algorithm which simulates accesses to the target components for all users in all possible roles counting the number of legal and illegal authorizations. The algorithm is performed twice, first on the before-attack system, second on the post-attack system.

- Case study illustration

The case study assumes users are assigned 4 roles: System administrator (Admin), Deposit services (Depos) and Loans services (Loan). The Database consists of three tables: Customers, Deposits and Loans. The Admin role is authorized to access all tables, The Depos role authorized to access to deposits tables, The Loan role is authorized access to loans table. Following the contents of Roles table (Table II) and Users table (Table III).

TABLE II. ROLES TABLE

ROLE	AUTHORIZATION
Depos	Deposits
Loan	Deposits, Loans
Admin	Customers, Deposits, Loans

TABLE III. USERS TABLE

User ID	Role
User1	Admin
User2	Depos
User3	Depos, Loans
User4	No
User5	No
User6	No
User7	No
User8	No
User9	No
User10	No

Following in Table IV the values of Confidentiality impact scores for all system components according to the normal authorizations, and also values of actual access permissions after a cyber-attack has occurred. Norm authorizations are according to legal authorizations' definitions. Actual permissions assumed number of illegal and lost permissions given after illustrating three kinds of cyber-attacks. At the rightmost column the evaluated CR according to Formula (1).

TABLE IV. CONFIDENTIALITY IMPACT EVALUATION

Attack Number	Components Table	Legal Norm	Legal Lost	ILegal Norm	ILegal Permitted	CR
1	Deposits	3	0	7	0	(0/3 + 0/7)/2 = **0**
1	Loans	2	1	8	5	(1/2 + 5/8)/2 = **0.56**
1	Customers	1	1	9	9	(1/1 + 9/9)/2 = **1**
2	Deposits	3	1	7	5	(1/3 + 5/7)/2 = **0.52**
3	Deposits	3	3	7	5	(3/3 + 5/7)/2 = **0.86**

VI. RESULTS

As illustrated, during attack number 1 Deposits table was not impacted by the attack, thus CR is zero. Customers table lost all user legal authorizations and in addition all illegal

users got permissions, thus CR is scored maximal hence 1. Loans table lost 1 users' permissions and 5 illegal users got permissions, hence the calculated CR is 0.56.

Comparing impacts of attack 2 on Deposits table to attack 1 on Loans table shows that although both attacks caused loss of access to one user and an addition of 5 illegal users, the calculated CR of attack 2 is less harmful (0.52 < 0.56). This is due to the fact that there are still 2 users having access to the table, while only 1 user has access to loans table.

Comparing impacts of attacks 2 and 3 on Deposits table shows that although the impacts on illegal users are similar, the impacts on legal number user is more harmful (0.86 > 0.52) in attack 3, since all legal users lost their access rights.

VII. CONCLUSIONS

This work presents a new framework of a Security Continuous Monitoring System, structure and mechanisms. The SCMS uses the CVSS scoring model for risk scoring operating in real time. According to the proposed model CVSS uses CR environmental parameters which are evaluated by the new algorithm, based on the technological configuration of the system, instead of CR figures which according to current practices, is based on users' personal intuitive knowledge. The structure of the system, modules and the scoring algorithm is presented and illustrated using a use case.

The model helps risk managers in estimating the organizational risks, basing their risk management decisions on the specific technological structure by using the algorithm. Using the proposed model will bring more accurate estimates to vulnerability risks, thus enabling efficient risk mitigation plans and improved defense strategies to organizations.

Confidentiality metric is used by risk scoring algorithm CVSS to measure the impact on confidentiality of a successfully exploited vulnerability.

The value of confidentiality score is calculated by using the basic parameter CI and the environmental parameter CR. Increased confidentiality impact raise the vulnerability score. CR metric enables customizing the CVSS algorithm to the importance of the affected IT asset to a user's organization. That is, if an IT asset supports a business function for which availability is most important, the metric will be assigned a higher value. CR has three possible values: "low," "medium," or "high". The proposed model presents an algorithm which enables assigning quantitative values to confidentiality impact based on the real planned and actual impact of an attack on the specific component. The calculated values are based on the actual impacts of cyber-attacks on that component, compared to the organizational needs as specified in the authorizations system. The formula and metrics are presented and illustrated in a use case example. The evaluated score is assigned real values instead of current qualitative estimates, thus enabling higher resolutions of confidentiality scores. The proposed model outlines the structure of a SCMS which uses the real organizational configuration, components, and processes. The model will enable getting more accurate measure, which are based dynamically on users' configuration thus enabling the organization making better risk management decisions, allocating risk management budgets to the relevant threats Incorporating the CR computed values in CVSS scoring model needs a minor modification to CVSS algorithm: using the calculated CR instead of the estimated values for all systems' components.

Future improvements to confidentiality impacts formulas and algorithm needs more research. Confidentiality impacts may be considerably elaborated in the following directions:

- Assigning different weights by the confidentiality formula to differentiate users who lost their access from un-authorized users who got illegal access.
- Assigning different weights to components according to business losses caused by attacks on the components.
- Assigning different weights to kinds of components such as software or hardware, operating system component or application components.
- Computing components' confidentiality score in relation to the amount of roles to a component a user is authorized, compared to the number of actual lost roles.
- Computing score according to the types of access a user is authorized in certain roles, for example differentiating between write and read access rights.
- Calculating scores according to the amount of interrelationships of the evaluated component with other components, measuring indirect impacts on other components, and including interrelationships' kinds such as reads or writes operations between components.
- Measuring impacts on types of users. Higher level organizational users and key personnel might be hurt more by loss of access then operational low-level workers.

More research is needed in supplying quantitative measures to the CVSS model. In our view CVSS model uses additional qualitative measures which could be improved adding quantifiable measures. Parameters such as target distribution may use the technological aspects of the configuration instead of users' intuitive estimates. Other environmental parameters such as integrity and availability scores should be based on figures representing the actual technological environment.

REFERENCES

[1] P. Mell, K. Scarfone, and S. Romanosky, "CVSS – A complete guide to the common vulnerability scoring system, version 2.0", 2007.

[2] L. Langer, "Stuxnet: dissecting a cyber warfare weapon, security and privacy", IEEE, Volume 9 Issue 3, pages 49-51, NJ, USA, 2011.

[3] S. Tom and D. Berrett, "Recommended practice for patch management of control systems", DHS National Cyber Security Division Control Systems Security Program, 2008.

[4] A. Terje and R. Ortwin, "On risk defined as an event where the outcome is uncertain", Journal of Risk Research Vol. 12, 2009.

[5] E. Weintraub, "Security Risk Scoring Incorporating Computers' Environment", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 7, No. 4, April 2016.

[6] Y. F. Nũez, "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.

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

[8] S. Harris, All in one CISSP Exam Guide. 6Th Ed. McGraw Hill Education, 2013.

[9] R. Sandhu, D. Ferraiolo and R. Kuhn", "The NIST Model for Role-Based Access Control: Towards A Unified Standard", George Mason Univ., 1999.

[10] M. G. Hardy, "Beyond continuous monitoring: threat modeling for real-time response", SANS Institute, 2012.

[11] A. Keller and S. Subramanianm, "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, 2009.

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

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

[14] I. Kotenko and A. Chechulin, "Fast network attack modeling and security evaluation based on attack graphs", Journal of Cyber Security and Mobility Vol. 3 No. 1 pp 27-46, 2014.

[15] FIPS Publication 199 - Federal Information proccessing standards publication, "Standards for security categorization of federal information and information systems", Department of Commerce, USA, February, 2004.

[16] E. Weintraub and Y. Cohen, "Continuous monitoring system based on systems' environment", ADFSL - Conference on Digital Forensics, Security and Law, Florida, USA, May 19, 2015.

[17] GAO – United States Government Accountability Office Report to Congressional Request, "Information security – state has taken steps to implement a continuous monitoring application but key challenges remain", July, 2011.

[18] E. Weintraub, "Quantitative measurement for estimation Confidentiality impacts after Cyber Attacks", ICSCT - International Conference on Secure Computing and Technology, Washington, USA, 11/2016.