Information & Computer Security

A comprehensive security control selection model for inter-dependent organizational assets structure

Maryam Shahpasand Mehdi Shajari Seyed Alireza Hashemi Golpaygani Hoda Ghavamipoor

Received 17 December 2013
Revised 30 May 2014
27 July 2014
14 August 2014
Accepted 18 August 2014

A comprehensive security control selection model for inter-dependent organizational assets structure

Maryam Shahpasand, Mehdi Shajari,
Seyed Alireza Hashemi Golpaygani and Hoda Ghavamipoor
Department of Computer Engineering and Information Technology, Amirkabir University of Technology (Tehran Polytechnic), Tehran, Iran

Abstract

Purpose – This paper aims to propose a comprehensive model to find out the most preventive subset of security controls against potential security attacks inside the limited budget. Deploying the appropriate collection of information security controls, especially in information system-dependent organizations, ensures their businesses' continuity alongside with their effectiveness and efficiency.

Design/methodology/approach – Impacts of security attacks are measured based on interdependent asset structure. Regarding this objective, the asset operational dependency graph is mapped to the security attack graph to assess the risks of attacks. This mapping enables us to measure the effectiveness of security controls against attacks. The most effective subset is found by mapping its features (cost and effectiveness) to items' features in a binary knapsack problem, and then solving the problem by a modified version of the classic dynamic programming algorithm.

Findings – Exact solutions are achieved using the dynamic programming algorithm approach in the proposed model. Optimal security control subset is selected based on its implementation cost, its effectiveness and the limited budget.

Research limitations/implications – Estimation of control effectiveness is the most significant limitation of the proposed model utilization. This is caused by lack of experience in risk management in organizations, which forces them to rely on reports and simulation results.

Originality/value – So far, cost-benefit approaches in security investments are followed only based on vulnerability assessment results. Moreover, dependency weights and types in interdependent structure of assets have been taken into account by a limited number of models. In the proposed model, a three-dimensional graph is used to capture the dependencies in risk assessment and optimal control subset selection, through a holistic approach.

Keywords Risk analysis, Risk management

Paper type Research paper

1. Introduction

Over the years, potential information security attacks have threatened businesses and their reputation. While emerging information systems and computer networks have been used to facilitate businesses, they remained vulnerable to hackers. Security managers have been trying to block the attacks, as much as they can, following the risk management (RM) process. RM is composed of two distinct procedures including *risk assessment* and *risk mitigation*. In the first procedure, risk of exploitations of asset

Information & Computer Security
Vol. 23 No. 2, 2015
pp. 218-242

2056-4961
DOI 10.1108/ICS-12-2013-0090

vulnerabilities is assessed based on related threats' occurrence likelihood and severity. Afterwards, security control selection is followed in the risk mitigation procedure. Despite RM's seemingly obvious procedure, in organizations with huge amount of interdependent information assets, it is a sophisticated process which not only demands high level of labor and budget but also does not often result in optimal solutions.

To make RM systematic, organizations like National Institute of Standards and Technology (NIST) and International Organization for Standards (ISO) have determined RM standards. In this regard, they have classified most of the experienced information threats and have introduced best plans, confronting the threats as countermeasures or security controls (Stoneburner *et al.*, 2002; ISO, 2008). However, considering and implementing the entire advised security controls may not be suitable or feasible for all organizations. As existing methods propose, determinant factors such as the assessed risk levels and action plan costs can define the priorities in decision making for security control selection. In most of these methods, simple risk management procedures are followed ignoring important factors such as asset interdependency or detail investigation into security criteria (CIA)[1]. Moreover, selecting the optimal subset based on control effectiveness considering the limited budget for security management has not been taken to account in such methods.

The model proposed in this paper finds the best subset of security controls, considering residual information risk and limited budget in information security management. In this regard, graph-based analysis is followed for risk assessment. On one hand, attack graphs are utilized to analyze assets' vulnerabilities which are needed to be exploited for a specific attack scenario. On the other hand, organizational asset dependency graph is devised to follow the impact of any vulnerability exploitation on the targeted asset and its dependent assets. Furthermore, to mitigate the assessed risk, a dynamic programming algorithm is proposed to reach out to the optimal subset of security controls inside the limited budget.

This paper presents the proposed model in the following structure. Related works are reviewed in Section 2, followed by the problem description in Section 3. The proposed control selection model is described in Section 4. An application example and the results for a real-scale model implementation are provided in Section 5. Final conclusions are discussed in Section 6.

2. Related works

More than 200 qualitative and quantitative methods have been proposed to simplify RM (Paintsil, 2012), such as CRAMM (Yazar, 2002), OCTAVE (Albert and Dorofee, 2003), CORAS (Soldal *et al.*, 2011) and MAGERIT (MFPA, 2012). Most of these methods imply the importance of considering the asset interdependencies in risk assessment and cost-benefit control selection, but only a few of them have formulated these objectives in a well-defined model. MAGERIT, for example, defined asset dependencies in two higher and lower asset levels. However, in this method, general threat impact diffusion among interrelated assets is defined without in-depth analysis of security criteria (CIA). Furthermore, MAGERIT utilizes ROI[2] for cost-benefit control selection analysis, which does not provide security analyzers with solution comparison capability when they are faced with limited budget (Demetz and Bachlechner, 2013). CRAMM also claimed that its asset model implies the risk propagation among interrelated assets. However, due to the lack of dependency weights and types, all the related assets affect

the dependent asset equally, which results in inaccurate risk amounts. To mitigate the risk, a comprehensive list of security controls with their priority factor is proposed to security analyzers by CRAMM. Although priority factor is used to sort the controls based on their importance, cost-benefit control selection and budget limitation have not been taken into account in this method.

To search for the cost-benefit security control portfolio, several combinations of computer science and mathematical techniques have been utilized so far. For example, Dewri *et al.* (2007, 2012) formulated attack trees through a multi-objective optimization problem and evolutionary algorithms. Other techniques such as security ontology (Neubauer *et al.* 2008) and heuristic algorithms like the multi-objective tabu search (MOTS) algorithm (Viduto *et al.*, 2012), the genetic algorithm (Rees *et al.*, 2011) and ant colony optimization (ACO) algorithms alongside with hidden Markov models (HMM) and dependency attack graphs (Zhang *et al.*, 2013) are also utilized with the same objective. Using evolutionary algorithms is reasonable for analyzing and searching big data when time is limited and finding local optimums is as good as the exact answer. But in security management, definite solutions are more desired than quick but not very accurate solutions. Rakes *et al.* (2012) have conducted a quantitative data set based on a threat set report, and proposed a model with respect to the given limited budget to find the optimal portfolio. Following Rakes *et al.*'s model, Sawik (2013) proposed a mixed integer programming model using the same threat report, taking advantage of two popular concepts in economics: value-at-risk and conditional-value-at-risk, to make the expert decisions more risk-aversive. However, none of the mentioned research works considered assets' operational interdependencies in RM.

To take organizational assets' relations and dependencies into account, a RM meta-model is proposed by Innerhofer-Oberperfle and Breu (2006), which combines the organization interdependent structure with the security management process, to handle the complexity of business supporting information processes. In Breu *et al.* (2008), authors used their previously proposed meta-model and defined interdependent organizational element categories, including IT infrastructure. They defined security requirements by an organizational dependency graph through a top-down approach from business objectives to technical security requirements and then mapped the objectives to goals which the attackers may target. Then, they assessed the risk through a bottom-up approach in the same graph. In another research, the asset-rank algorithm inspired by the Google page-rank algorithm is presented to identify critical assets based on their impacts on other assets (Sawilla and Ou, 2008); however, they did not mention any solutions for control selection. Alpcan and Bambos (2009) used a risk-rank formula to calculate the propagated risk amount among dependent risk element supersets. Mounzer *et al.* (2010a, 2010b) mapped the security control selection problem to a Markov decision process and used the risk-rank formula to propose the best control portfolio, with respect to asset dependencies. However, technical assets such as servers or network equipment were not discussed in their model. In their next research, Mounzer *et al.* (2010a, 2010b) used asset dependency graphs to follow the risk propagation on assets. In this approach, dependency graph features will be changed after implementing security controls, which forces dynamic changes in graph structure.

3. Problem definition

As discussed, the optimal subset out of all the recommended security controls is desired. In this regard, a measurement method for control comparison is needed. As the security control objective is to mitigate the risk of security threats, control effectiveness is defined as the amount of risk that is supposed to be mitigated by this control. But, at the first step, the risk level on each asset must be assessed. Regarding these issues, the focus of this paper is the answers to the following questions:

- How to analyze the risk to be able to measure the control effectiveness?
- How to measure the control effectiveness?
- By having controls effectiveness, how to select the best subset of security controls inside the limited budget?

To explain the model, the notations provided in Table I are used in the rest of this paper.

Indices	
T	= threat, $t \in T = \{1, \ldots, r\}$
C	= security control, $c \in C = \{1, \ldots, n\}$
A	= asset, $a \in A = \{1, \ldots, o\}$
K	= chosen security controls, $k \in K, K \subseteq J = \{1, \ldots, n\}$
Av., Int., Conf.	= security criteria, "Av.", "Int." and "Conf." stand for "Availability", "Integrity" and "Confidentiality" respectively.
Input parameters	
$V(a) = \langle V_{Av.}(a), V_{Int.}(a), V_{Conf.}(a) \rangle$	= Intrinsic value of the ath asset, how much value this asset has? How much loss we would have if each of these criteria gets violated?
$DIm(t,a) = \langle DIm_{Av.}(t,a), DIm_{Int.}(t,a), DIm_{Conf.}(t,a) \rangle$	= Direct Impact, the impact of tth threat if it turns to an attack on ath asset, $\in [0,1]$, e.g. <-, 0.5, 1>
1_1_DT(a,a')	= One-to-one dependency type $\in \{Linear, Amplified\}$*
1_M_DT (1_1_DT (a_α,a_β), …,1_1_DT (a_λ,a_δ))	= One-to-many dependency type $\in \{Conjunctive - maximum, Conjunctive - summation, Disjunctive, Threshold\}$; $\alpha, \beta, \lambda, \delta \in A = \{1, \ldots, o\}$
IDM(a, a') = $\begin{pmatrix} ID_{(Av.,Av.)}(a,a') & ID_{(Av.,Int.)}(a,a') & ID_{(Av.,Conf.)}(a,a') \\ ID_{(Int.,Av.)}(a,a') & ID_{(Int.,Int.)}(a,a') & ID_{(Int.,Conf.)}(a,a') \\ ID_{(Conf.,Av.)}(a,a') & ID_{(Conf.,Int.)}(a,a') & ID_{(Conf.,Conf.)}(a,a') \end{pmatrix}$	= Impact Diffusion Matrix, the amount of defect that propagates from a to a' , due to dependency of a' to a ,when an attack episode takes place on a
Cost (c)	= Cost of security control c implementation
Prop(t,c)	= Proportion of tth threat that will be blocked directly if control c is implemented
p(t)	= Probability of tth threat occurrence
B	= Available budget for security hardening

Note: *Dependency types are discussed in section 4.3.1

Table I. Notation

4. Control selection model

Questions previously discussed are answered through the proposed comprehensive model. As the main contribution of this paper, control features (effectiveness and cost) are added to a graph-based model of organizational assets and their related risks with the objective of finding cost-benefit control portfolio. The significant outcome is the ability to capture the mitigated risk on interdependent asset structure. By using the algorithm in the following sections, security managers would be able to assess the effectiveness of each security control portfolio, based on accurate risk assessment results.

The overview of the model is presented in Figure 1. Abbreviations used in this figure are defined in Table I. *Risk assessment* and *control selection,* as the main parts of this model, are explained in detail in the following sections.

4.1 Graph-based risk assessment model

Risk assessment starts with investigation into organizational assets and possible attacks that threaten these assets' security criteria. Technical assets have vulnerabilities which are listed in NVD[3] and coded by CVE[4], having their probable severity of exploitation calculated by CVSS[5] (Mell *et al.*, 2007). When an attack scenario starts, it may target one or more vulnerabilities of assets in its way (i.e. attack path; Sheyner, 2004). Following the steps in each attack path, the related risk is assessed, while the direct and indirect impacts of each attack step on interdependent assets are considered. The following graphs are formulated with the objective of risk calculation:

- *Organizational Dependency Graph: ODG: <A, E, V, IDM>*. ODG is an acyclic directed graph which represents organizational structure and propagation of attacks' impact between assets. *A* is the set of organizational assets as graph

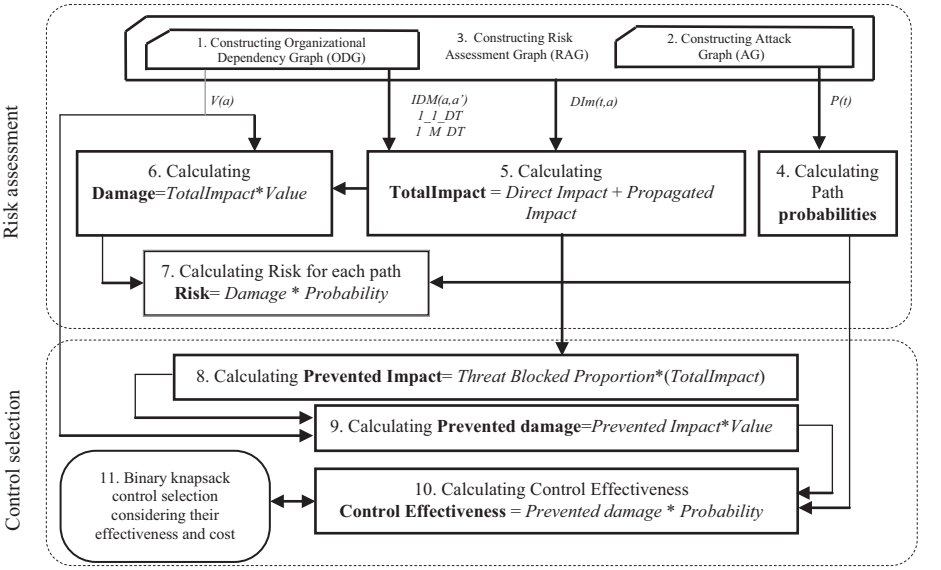

Figure 1.
Security control selection model for interedependent assets' structure

Notes: Bold and italic words represent each step output and input, respectively

nodes, labeled with their intrinsic values (defined as $V(a)$ in Table1). E ($\subset A*A$) is the set of edges between asset nodes representing their dependencies, labeled with *impact diffusion proportion* (having this value as *IDM* in Table I).

- *Attack Graph: AG: <S, E', P>*. AG is an acyclic directed graph that represents the attack states and paths based on assets' vulnerabilities and their related threats. S is the set of attack states as graph nodes, including *initial states* (S_I) where the attack starts and *goal states* (S_F) where the attacker gains what he was looking for. These states are about the results of threats (set T in Table I) being realized. E' ($\subset S*S$) is the set of edges (i.e. attack steps) between attack state nodes as the transition between vulnerabilities through an attack path, labeled with P as probability of an attack step. This graph also shows vulnerability dependencies; such that in an attack path, some sorts of exploitations are needed to gain a specific goal.
- *Risk Assessment Graph: RAG: <AG, ODG, E", DIm>*. RAG represents all vulnerability exploitation impact per each attack step over the organization's assets. AG includes attacks' paths and their probabilities, and ODG represents attacks' impact diffusion on interdependent assets. E" maps the vulnerability that has been exploited in each step in AG to each asset node in ODG and labeled with Direct Impact of these threats' realization (defined as *DIm(t,a)* in Table I).

The schematic of RAG is presented in Figure 2. The automated or manual generation of these graphs is out of the scope of this paper; however, they are utilized to propose a holistic approach for security control selection.

In this model, the value of assets and types and weights of dependencies among assets are considered as risk calculation fundamentals. Details about ODG elements, their valuation method and different types of their dependencies are discussed in the following subsections.

4.1.1 Interdependent structure of organizational assets. The assets are divided into the following categories based on Breu *et al.*'s (2008) definitions:

- OU: *Organizational Units*, the enterprise as a whole, business units or departments.

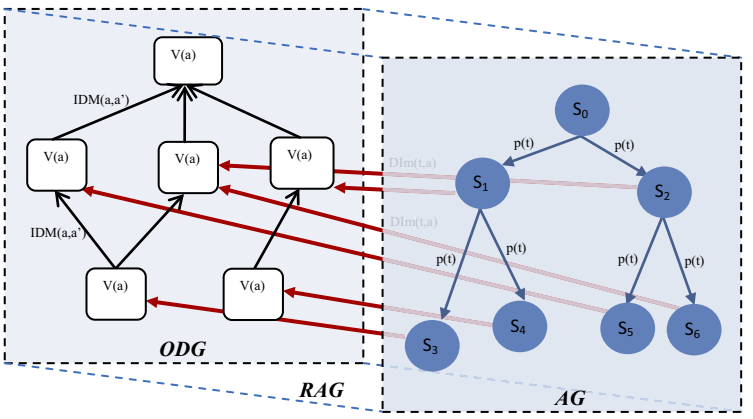

Figure 2.
Risk assessment graph

- BP: *Business Process*, as a sequence of activities which are followed to accomplish a goal.
- R: *Roles*, as sets of responsibilities imposed on an employee who plays this role in the organization.
- I*: *Information Objects*, as the information that is used by *Business Process*.
- C*: *Components*, are the applications such as business software and Web services used by business processes.
- N*: *Node*, as software and hardware set which provides all the required services for components to operate or information objects to be stored (Windows Server, 2003 installed on a PC) (* presents assets that are faced with direct security threats).

A modified version of Breu *et al.*'s meta-model with asset relations and dependencies is shown in Figure 3(a). An extra element "*Edge*" is added to this meta-model, which stands for transformation media such as routers, switches, cables, etc. Model elements are classified in three layers: business, application and technical[6]. The dependency graph, based on this meta-model, is shown in Figure 3(b).

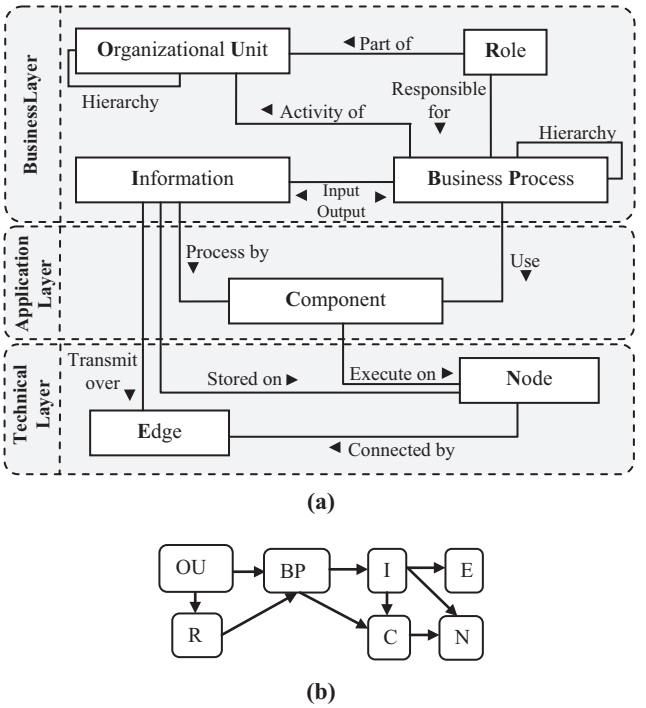

Figure 3.
Modeling asset dependencies

Notes: (a) Interdependent organizational structure meta-model; (b) model elements dependency graph

4.1.2 Asset valuation. The value of assets is defined as its providence cost and the profit that it brings into the organization business (Stoneburner *et al.*, 2002). Many standards and research works have defined IT asset valuation methodologies (Poore, 2000; Moody and Walsh, 1999; Eom *et al.*, 2005; ISO, 1998; BritishStandard, 2006). In this paper, summation of the following items is used, which are depicted to security criteria as V (a) in Table I:

- costs of providing and maintaining desired level of CIA;
- potential loss of profit through CIA compromise; and
- law/reputation penalty costs through CIA compromise.

Notice that CIA are reasonable for the asset types, as presented in Table II. So, it is possible to have "−" value which stands for "not defined value" for some criterion in *V (a)* vector. To explain this valuation approach with an example, consider an operational asset like accounting software in an organization. Assume that the organization has paid $2,000 for this software and it cuts $200 of costs each month. Moreover, if the software's integrity is compromised in a way that would result in calculating wrong numbers (lower than the right amount) for employee's salary, the organization should pay them their salary and 5 per cent more as the penalty. For instance, if the organization has 20 employees with $100 salary per month, the intrinsic value of this asset in a one-year period would be (in *V (a)* format presented in Table I): <$2,000 + 12($200), 12 × 20 × 5 per cent($100), - >.

4.1.3 Dependency types. Another important issue is about details of dependency types in the *ODG* graph for operational dependencies. The final impact is calculated based on type and weight of dependencies (having these values in *1_1_DT*, *1_M_DT* and *IDM* in Table I). In Jahnke *et al.* (2007), availability dependency types were discussed to calculate the cascaded proportion of impacts due to dependencies among nodes. Expanding these types to all security criteria has led to the following two types of dependencies in the proposed model:

(1) One-to-one dependencies.
The impact propagates directly from asset *a* to asset *a'* in one of the following three ways:
   - *Linear propagation*: If *IDM(a,a') < 1*, it means the impact of each threat realization on *a'* is a proportion of direct impact of that threat realization on *a*. For example, if the electronic payment system is broken, the electronic commerce system will be linearly broken too.
   - *Amplified propagation*: If *IDM(a,a') > = 1*, with respect to each threat realization direct impact on *a*:

CIA	Information	Components	Other model elements
Confidentiality	✓		
Integrity	✓ (depends on components integrity)	✓	
Availability	✓ (depends on components and hardware availability)	✓ (depends on nodes availability)	✓

Table II. CIA defined for assets

- *a'* will be affected completely if (*1/ IDM (a,a') >= DIm(t,a)*); and
- *a'* will be affected equal to proportion of the diffusion impact from *a,* if (*1/ IDM (a,a') < = DIm(t,a)).*

An example of the first case can be: disclosure of users' login table that contains username/password information, which would result in all accounts' privacy disclosure.

(2) One-to-many dependencies.

An asset may be affected by several other assets; the total impact due to these dependencies is calculated through one of the following types:

- *Conjunctive*:
  - *Maximum*: If an asset is dependent to many other assets simultaneously, the final impact is the maximum amount it could get from the related assets; for example, consider a Web site which uses a Web server and a database server simultaneously; if attackers compromise both servers, the impact on Web site would be equal to the maximum impact on the two servers.
  - *Summation*: If an asset is dependent to many other assets separately, it gets the summation of all impacts. For example, consider operational information which is saved with 50, 30 and 20 per cent proportions on database, PC#1 and PC#2, respectively. If attackers compromise all of the assets, the impact on information would be equal to the summation of impacts.
- *Disjunctive*: If an asset is dependent to many other assets, in which it could operate even when there is only one asset which has remained uncompromised, if all of assets break, the final impact would be the minimum possible impact. Assume the same Web site, which is now dependent on two database servers, which serve the same information as mirrors. If attackers compromise both of the servers, the impact on the Web site would be equal to the minimum impact.
- *Threshold*: If asset *a* is dependent to *m* assets, and if *n* assets out of these *m* assets break, *a* will break completely. For example, in a system with a shared key approach for users' authentication, if passwords of *n* users out of *m* users are reached, the attacker can access the entire system.

By capturing all types of propagation for attack impacts, the risk can be assessed using the basic formula for risk assessment: "Risk = Asset Value × Attack Impact × Attack probability". Controls must be selected according to the current risk level. This selection should be based on the control features which are presented in the next section.

4.2 Control feature definition

Measurable metrics for security controls should be defined for their comparison. In the proposed model, *security control effectiveness* and *cost of implementation* have been defined with respect to the mentioned measurable metrics.

To assign an effectiveness score to each control, target threats and assets should be understood thoroughly. Some controls are defined as fundamental controls, such as *risk assessment policies*, *software/hardware inventory management* or *security training courses for employees*. Although these controls do not directly prevent any attacks, they are the preconditions for security management. As a result, we consider these controls

as pre-selected controls and their implementation cost will be subtracted from the total budget. Moreover, security controls may be applied in different ways such as disconnecting the vulnerable asset from threat sources, disabling specific connectivity features, patching the asset vulnerability or configuring new security technologies and devices (Zhang *et al.*, 2013). Regardless of these options, in this model, preventing the exploitation of vulnerability is considered as the control objective and control effectiveness is defined as its success rate.

There are many models and approaches to measure the security control effectiveness (Torres *et al.*, 2006; Hagen *et al.*, 2008; Boehmer, 2008; Liu and Zhu, 2009). All of these models believe that security controls cannot mitigate the total amount of probable risks. Hence, it is reasonable to estimate a proportion of risk mitigation for each control. Table III shows an example of such estimation which is defined as *Prop (t, c)* in Table I.

In this table, assume Threat#1 is about viruses through computer networks. SC#1 implies authentication considered for installing new software which denies 99 per cent of unauthorized accesses, SC#3 implies anti-virus software installation on all computers which prevents 95 per cent of this threat realization and SC#2 that is not devised to prevent Threat#1 realization. This estimation could be even qualitative and in verbal terms such as "high, medium, low" based on security team preferences.

In addition to effectiveness, the control implementation cost should be defined and measured. This could be as easy as using the summation of the *installation costs* ($), *operation costs* ($), *system downtime* (hrs), *incompatibility costs* (scale) and *training costs* ($) for each control (Poolsappasit, 2010).

4.3 Control selection model

The proposed risk assessment model enables security analyzers to follow the impact of a threat realization on interdependent assets. By adding control features to this model, it can be assumed that attack graph nodes are labeled with security controls. This labeling helps us follow the preventive power of each control on organizational interdependent structures. Figure 4 illustrates this issue.

Figure 4 shows that an attack can be prevented by many controls; also, a control can prevent many attacks simultaneously. Regarding this issue, control effectiveness must be calculated, such that when a control is chosen for implementation, the effectiveness of new controls should be calculated per the proportion of attacks, which the chosen

Table III.
Example of security control effectiveness estimation

Descriptions/indexes	Security control no. 1	Security control no. 2	Security control no. 3
Threat number 1	0.99	0	0.95

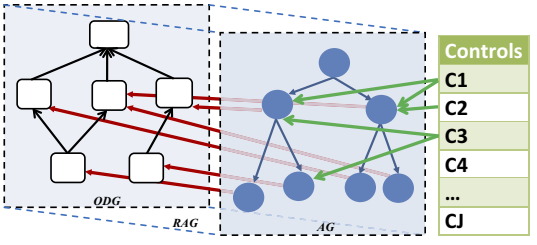

Figure 4.
Mapping controls to related realized threats

controls had not prevented. Furthermore, an important assumption in this calculation is that each attack path occurs independently and nodes' failure is considered separately for each path. In other words, for a common step in two different attack paths, the damage of this step for the first path will be calculated, such that the other path has not been realized or has been realized and repaired before the first path's occurrence. Therefore, assets are considered in their uncompromised state at the beginning of each path.

Following knapsack idea in picking the most valuable set of objects, Shahpasand and Hashemi (2013) proposed a dynamic programming algorithm to find the optimal security control portfolio. They mapped control effectiveness and its implementation cost to item features and the limited budget to the limited knapsack capacity. Inspired by their algorithm, an algorithm is presented in Figure 5, which finds the optimal control portfolio based on their effectiveness.

This algorithm covers Steps 9,10 and 11 in the proposed model in Figure 1. The structure of *RAG* (including *AG* and *ODG*), number of controls (*n*) and their related cost of implementation [*Cost(c)*], the prevention proportion of each attack episode by each control [*Prop(t,c)*] and available budget (*B*) are taken as inputs in this algorithm. The loop "*For*" in Lines 9 to 11 prepares matrix "*m*", which keeps the maximum value in each state in dynamic programming. The second loop "*For*" in Lines 13 to 17 prepares matrix "*Selection[]*" with "0" initial values, which is about the decision in each step. This matrix is mandatory, because for calculating control effectiveness, the implementation state of other security controls is required. As aforementioned, "*DIm*" of a threat (*t*), that remains after a control (*c*) implementation, would decrease to "*Prop(t,c)* DIm(t)*"; as a consequence, the effectiveness of other controls should be calculated for the remaining threat impact proportion called "*DIm'*".

From the 21st line, the algorithm starts to complete matrix "*m*", row-by-row, for each control. In Lines 23 and 24, matrix "*Selection[]*" changes its upper-half rows (which is about $c\text{-}1^{th}$ control status) with its bottom-half rows [which is about c^{th} control status per different amount of money (0 to budget)] and puts "0" for all of the bottom-half rows, which is about the new decision for $c+1^{th}$ control (in each step in loop "*For*" that starts at Line 26). This exchange happens on each *c* index.

Loop "*For*", which starts at Line 26, is about two possible states of control selection. If the control cost of implementation is lower than the available budget in each state of "*money*", the algorithm checks whether adding this control makes the portfolio more effective (Line 48) or having the same portfolio would result in more effectiveness (Line 51). Otherwise, if its cost is more than the remaining budget, it will continue with the same portfolio in the previous row of matrix "*m*" (Line 54 to 57).

The contribution which is discussed before is the calculations provided in Lines 30 to 44. In this part, the direct impact of each threat realization (*DIm*) is defined as "*DIm'*" to capture the blocked proportion of attacks per c^{th} control. For all of the controls selected in the previous state (controls in set *K*), the remaining proportion of attacks that c^{th} control is going to block, must be calculated. For a node in AG that c^{th} control has targeted, the remaining attack proportion should be calculated, if there is any other chosen control that has targeted this node (Lines 32 to 36). The effectiveness of c^{th} control should be considered through any path that contains the related threat node – which is equal to the prevented damage through that path multiplied by path

```
1   // Input:
2   // Number of Controls (n)  and their Implementation Costs on each asset (Cost[c])
3   // Number of Threats (r)
4   // limited budget (B)
5   //Proportion of Threat t that will be blocked if Control c is implemented (prop[t,c])
6   //RAG, having AG's information(DIm and paths' probabilities)and ODG's information(IV and IDM)
7   ================================================================================================
8   //PREPARING MATRIX "m" IN DYNAMIC PROGRAMMING FOR FILLING IT STEP BY STEP IN MAIN FOR LOOP
9   For (money from 0 to B) Do
10    m[0, money] := 0;
11  End For //(line 9)
12  //PREPARING SELECTION MATRIX, IT'S ROWS REPRESENT THE DECISION FOR CONTROL SELECTION ON EACH STATE
13  For (b from 0 to B) Do
14  For (c from 1 to n)Do
15        Selection[b,c] := 0 ;
16  End For //(line 14)
17  End For //(line 13)
18
19  //FILLING MATRIX "m" STEP BY STEP PER EACH CONTROL FROM "1" TO "n"(ROWS) AND  AMOUNT OF BUDGET
20  //STARTING FROM "1" TO B (COLUMNS)
21  For (c from 1 to n) Do
22    // KEEPING THE PREVIOUS ROW DECISIONS FOR NEW ROW (EACH ROW BELONGS TO A CONTROL IN MATRIX "m")
23    Selection [1:(B),all] := Selection[(B+1):2*B,all];
24    Selection[B+1 : (2*B),all] := 0;
25
26    For (money from 0 to B) Do
27      If  (money >= cost[c]) Then
28  //CALCULATING CONTROL EFFECTIVENESS ACCORDING TO THE PRESENT SUCCESSFUL THREATS' PROPORTION       //
29  AND OTHER CONTROLS STATE OF IMPLEMENTATION
30        DIm':=DIm ;
31        K := all controls selected in "money-cost[c]" row of "Selection" matrix;
32        For (all Controls in K such as k)
33          If (any node in AG(such as threat t)corresponds to k^th Control, is common with control c)Then
34                DIm'[t]:= DIm'[t] * prop[c,k];
35          End If //(line 33)
36        End For //(line 32)
37        effectiveness[c]:=0;
38        For (t from 1 to r) Do
39            For (all paths in AG that includes node t that correspond to c^th Control) Do
40               Prevented_Damage[c]:= Calculate Damage(from node t to the end of path in ODG by DIm') *
41                                     prop[t,c];
42               effectiveness[c] := effectiveness[c]+ (Prevented_Damage[c] * Path Probability);
43            End For //(line 39)
44        End For //(line 38)
45
46        m[c, money] := max(m[c-1, money], m[c-1, money-cost[c]] + effectiveness [c]);
47
48        If (m[c-1, money - cost[c]] + effectiveness [c]> m[c-1, money]) Then
49           Selection[B+ money, all] := Selection[money - cost[c], all];
50           Selection[B+ money, c] :=1;
51        Else
52           Selection[B+ money, all] := Selection[money, all];
53        End If //(line 48)
54      Else
55        m[c, money] := m[c-1, money];
56        Selection[B+ money, all] := Selection[money, all];
57      End If //(line 27)
58    End For //(line 26)
59  End For //(line 21)
```

Figure 5.
Dynamic programming algorithm pseudo code for control selection

probability (Lines 38 to 44). The total effectiveness of this control would be the summation of its prevention through all of the related paths (Line 40).

To increase the transparency in damage calculation, the "**Calculate Damage**" phrase is used in Line 40 and its steps are explained in the following:

- Find all the steps in AG that t^{th} threat participates in.
- Through RAG edges between AG and ODG, find the node (asset) that t^{th} threat corresponds to that node's vulnerability by *DIm*.
- Having *DIm* for t^{th} threat's realization, *1_1_DT* and *1_M_DT* for dependency types and matrix *IDM*, calculate total (direct and indirect) impact of t^{th} threat's

realization (*TI[t]*) on each asset based on dependency types discussed in Section 4.1.3.

- Having assets' values [*V(a)*], calculate the damage of t^{th} threat's realization on each asset by *Damage(t) = V (a) * TI (t)*.

5. An application example and a real-scale evaluation

In this section, the application of the proposed model is discussed through an example. A small set of interdependent assets and security controls illustrates the model steps in practice. Furthermore, results for a real-scale implementation of the model are discussed.

5.1 An application example

Consider an organization with the structure shown in Figure 6. This organization develops software through two main business processes: "BP1: Produce" and "BP2: Sales and Marketing". "R1: Programming Team" as BP1's roles work with "I1: Products Information" such as products' codes and documentations, instructions, production analysis plans, etc. using "C3: File Management Software" running on a "N3: File Server" and "C4: Programming Tools" running on "N4: Internal Network Computers". There is only one "R2: Sales Manager" role who manages sales through a sale "C1: Sale Web Application" running on a "N1: Web Server". "R2: Sales Manager" also works directly with "I2: Sales Information" through "C3: File Management Software". "C1: Sale Web Application" and "C3: File Management Software" are both dependent to "C2: DBMS" for their operation. Dependency rates are about impact propagation among dependent assets.

Servers are accessible in three ways: programming team can only access "C3: File Management Software" through "N4: Internal Network Computers"; "R2: Sales

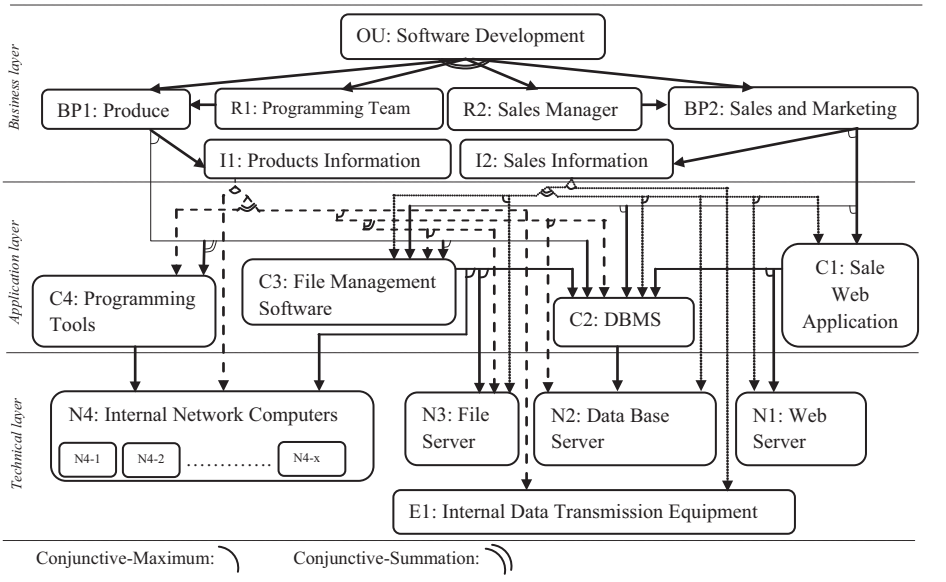

Figure 6.
Example of an interdependent organization structure (Step 1 in proposed model)

Manager" can access "C2: DBMS" and "C3: File Management Software" through "N4: Internal Network Computers" and through Internet with trusted external personal computers that access "C2: DBMS" by "C1: Sale Web Application"; and costumers only can access "C2: DBMS" by "C1: Sale Web Application" through Internet with personal computers to buy products. External computers such as customers' computers are not considered as organizational assets, but as reports indicate, about 92 per cent of attacks start from external sources (Verizon, 2013); they also should be included in the risk assessment graph as attack sources.

It should be noted that the dependency graph does not represent accessibilities, it is just about operational dependencies among graph elements, which can result in impact propagation. The propagated impact goes the reverse path in dependency graph; for example, file management software is dependent to the file server as a node, if the file server experiences an impact, dependent assets such as file management software will also face a propagated impact due to its dependency to the file server.

Assume all dependency types are linear, and one-to-many dependencies are *Conjunctive* (maximum and summation, as presented in Figure 7). The following tables include the information which is needed for constructing RAG.

Simple attack paths are provided in this example and required preconditions about each attack step are excluded. In this order, 12 vulnerabilities of the technical assets and related security controls which can mitigate the risk of these vulnerabilities are presented. The numbers in NVD, which are normalized and modified by experts, are used for impact vector and the probability of occurrence (exploitability) for each threat. For example, direct impact of vulnerability CVE-2003-1329 exploitation is estimated "<1,1,1>"[7] in NVD; but in this example, the vulnerability refers to network computers, which their *integrity* and

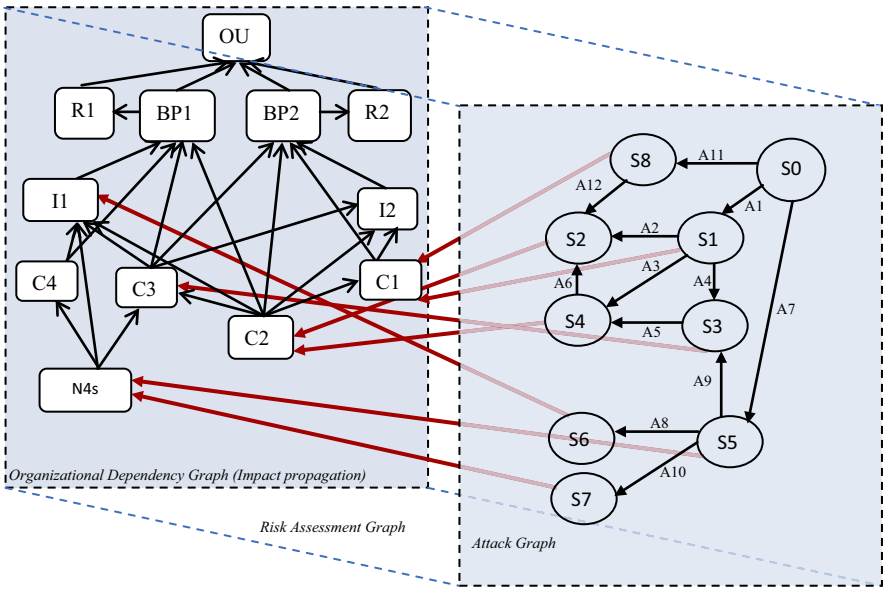

Figure 7.
Risk assessment graph and its sub-graphs (Steps 1, 2 and 3 in proposed model)

confidentiality as a hardware are not defined in Table II. As a result, we have considered "<1,-,->" for the direct impact of this vulnerability exploitation. The dependency weights (stored in *IDM* in Table I) on ODG are defined by experts who have complete knowledge about organization's structure.

Considering information provided in Table IV, *AG* would be a sub-graph of *RAG*, as presented in Figure 7. To make the graphs less complicated, only assets that are involved in risk assessment, due to their dependencies, are shown. Utilizing this graph, the risk of exploitation of vulnerabilities presented in Table IV can be assessed for seven possible attack paths, which are presented in Table V. For each path, respective damage is calculated for each node in ODG and multiplied to attack step probability in that path in Table V. The probability of each step is simply calculated by multiplying its probability to its previous steps' probability.

Security controls related to these threats listed in Table VI; and their implementation cost and preventive power are presented in Table VII (this table is similar to what has been discussed in Section 4.2). A specific form of Figure 4 for this example is shown Figure 8. As discussed in Section 4.3 and shown in Figure 8, there are several controls for each threat; but, for the sake of simplicity, we have just considered one control as a representative of all possible applications of this control in Table VII.

To explain risk calculation for each step, consider attack "A6" as an exploit for second vulnerability in Table VI; there are three different paths which end to this attack step:

- (A1, A3, A6) → probability: 0.648
- (A1, A4, A5, A6) → probability: 0.6269
- (A7, A9, A5, A6) → probability: 0.6561

For each path, different risks will be calculated and their summation results in the risk amount. Remember, it is assumed that each attack path happens separately and in initial system state, where no damage is occurred. Moreover, this step occurred after other steps, which means the related damage will be different due to different impacts related to pervious steps. So, having direct and propagated impact for this threat and dependent assets' values, the damage of this attack for each path will be:

- The damage A6 caused in (A1, A3, A6) → 3.7939
- The damage A6 caused in (A1, A4, A5, A6) → 2.5
- The damage A6 caused in (A7, A9, A5, A6) → 5.5107

And the related risk will be:

(3.7939* 0.648) + (2.5* 0.6269) + (5.5107* 0.6561) = **7.6412**

The following table shows different control portfolios per different available budgets. Notice that, the cost of implementation for fundamental controls discussed in Section 4.2 is subtracted from initial budget.

Table VIII shows that the algorithm proposes the best subset in each situation. The total risk calculated for these scenarios is *49.75167583,* as presented in Table V. If all the advised controls in Table VI are implemented, *43.3624* amount of the total risk will be prevented. This is reasonable, as controls cannot prevent all the probable attacks. The most significant observation is that, in some cases, even by investing more money, the mitigated risk had a very slight or no increase. For example, notice the row with

Organizational dependencies information			
Model elements		Intrinsic Value of Assets: $IV(a)=< IV_{Av.}(a), IV_{Int.}(a), IV_{Conf.}(a)>$ (10^3(K)$ in one year period)	Impact propagation due to operational dependencies: Impact Diffusion Matrix(a, a')= $\begin{pmatrix} ID_{(Av.,Av.)}(a,a') & ID_{(Av.,Int.)}(a,a') & ID_{(Av.,Conf.)}(a,a') \\ ID_{(Int.,Av.)}(a,a') & ID_{(Int.,Int.)}(a,a') & ID_{(Int.,Conf.)}(a,a') \\ ID_{(Conf.,Av.)}(a,a') & ID_{(Conf.,Int.)}(a,a') & ID_{(Conf.,Conf.)}(a,a') \end{pmatrix}$
OU		Organizational Units have no Intrinsic value and will receive the propagated damage from Roles and Business Processes.	
Business Processes: No Intrinsic value	BP1	Business Processes have no Intrinsic Value and just propagate the received propagated impact from Information and Components to Roles and propagate received damage to Organizational Units.	$(C2, BP1)=\begin{pmatrix}0.2 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(C3, BP1)=\begin{pmatrix}0.3 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(C4, BP1)=\begin{pmatrix}0.5 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(I1, BP1)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
	BP2		$(C1, BP2)=\begin{pmatrix}0.8 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$ $(C2, BP2)=\begin{pmatrix}0.8 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(C3, BP2)=\begin{pmatrix}0.2 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(I2, BP2)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
Information : Creation costs + potential loss of profit + Low/Reputation penalty cost	I1	<4,1, 2.5>	$(C2, I1)=\begin{pmatrix}0.2 & - & - \\ - & 0.2 & 0.1 \\ - & - & -\end{pmatrix}$,$(C3, I1)=\begin{pmatrix}0.3 & - & - \\ - & 0.3 & 0.6 \\ - & - & -\end{pmatrix}$,$(C4, I1)=\begin{pmatrix}0.5 & - & - \\ - & 0.5 & 0.3 \\ - & - & -\end{pmatrix}$, $(N4, I1)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(N2, I1)=\begin{pmatrix}0.2 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(N3, I1)=\begin{pmatrix}0.3 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(E1, I1)=\begin{pmatrix}0.5 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
	I2	<1, 2, 2>	$(C1, I2)=\begin{pmatrix}0.8 & 0.8 & - \\ - & 0.8 & 0.5 \\ - & - & -\end{pmatrix}$,$(C2, I1)=\begin{pmatrix}0.8 & 0.8 & - \\ - & 0.8 & 0.5 \\ - & - & -\end{pmatrix}$,$(C3, I2)=\begin{pmatrix}0.2 & - & - \\ - & 0.1 & 0.5 \\ - & - & -\end{pmatrix}$, $(N3, I2)=\begin{pmatrix}0.2 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(N2, I2)=\begin{pmatrix}0.8 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(E1, I2)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
Roles: Salary	R1	<3, -, ->	$(BP1, R1)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
	R2	<2, -, ->	$(BP2, R2)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
Components: Purchasing costs + potential loss of profit + Low/Reputation penalty cost	C1	<1, 1, ->	$(N1, C1)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(C2, C1)=\begin{pmatrix}0.25 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
	C2	<3, 2, ->	$(N2, C2)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
	C3	<0.5, 0.5, ->	$(N3, C3)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(C2, C3)=\begin{pmatrix}0.35 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$, $(N4, C3)=\begin{pmatrix}0.95 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
	C4	<0.2, 0.05, ->	$(N4, C4)=\begin{pmatrix}1 & - & - \\ - & - & - \\ - & - & -\end{pmatrix}$
Edges and Nodes : Purchasing and maintaining cost	N1	<2, -, ->	(No dependency and no propagated impact are defined for this asset)
	N2	<4, -, ->	(No dependency and no propagated impact are defined for this asset)
	N3	<1, -, ->	(No dependency and no propagated impact are defined for this asset)
	N4	<0.1, -, ->	(No dependency and no propagated impact are defined for this asset)
	E1	<1, -, -> (all the transmission media)	(No dependency and no propagated impact are defined for this asset)

Assets' vulnerabilities information based on NVD and (Mell, Scarfone & Romanosky. 2007) (steps 4.1 and 4.2 in proposed model)

Victim	Attack step	CVE #	Vulnerabilities needed to be exploited	Exploitation Direct Impact: $DIm(t,a)=< DIm_{Av.}(t,a), DIm_{Int.}(t,a), DIm_{Conf.}(t,a)>$	Probability of occurrence for each step in genereal
C1	A1	CVE-2002-0364	Chunked Code Buffer Overflow	<0.5,0.5,->	0.9
C2	A2	CVE-2003-0095	Unauthorized Remote to Root Privilege Login	<1,1,->	0.9
C2	A3	CVE-2009-1978	Unauthorized Remote to User Privilege Login (C1 to C2)	<0.5, 0.5, ->	0.8
C3	A4	CVE-2007-4909	Unauthorized FTP Remote to User Privilege Login(C1 to C3)	<1,1,->	0.86
C2	A5	CVE-2002-0965	Unauthorized FTP User to SQL User Privilege Login	<0.5, 0.5, ->	0.9
C2	A6	CVE-2008-1668	Oracle TNS Listen Buffer Overflow	<1,1, ->	0.9
N4	A7	CVE-2013-6798	Unauthorized Remote to User Login to Internal Computers	<0.05,-,->	0.9
I1	A8	CVE-2011-0030	Copying Products' Analysis Plans	<-, -, 0.3>	0.34
C3	A9	CVE-2003-1329	DOS Through FTP	<1,-,->	0.9
N4	A10	CVE- 2010-0023	Setup Processing Viruses Through Network	<1,-,->	0.34
C1	A11	CVE-2008-2384	SQL Injection	<0.5,0.5,->	0.9
C2	A12	CVE-2007-6304	DOS Through SQL	<0.5,-,->	0.9

Table IV.
Risk assessment information (input parameters)

Table V.
Total impact = direct impact + propagated impact for each attack path and related risk (Step 5, 6 and 7 in proposed model)

Descriptions/ indexes	Attack paths (A1, A2)	(A1, A3, A6)	(A1, A4, A5, A6)	(A7, A8)	(A7, A9, A5, A6)	(A7, A10)	(A11, A12)	
ODG nodes				**<-,-,0.3>**				
I1	<0.305,0.2, 0.1>	<0.305,0.2, 0.1>	<0.5, 0.5, 0.7>	<0.05,-, ->	<0.525,0.2,0.1>	<1,-,->	<0.1525-, ->	
I2	<0.87,0.8, 0.5>	<0.87,0.8, 0.5>	<1,1, 1>	<0.01425,-, ->	<1,0.8, 0.5>	<0.285,-, ->	<0.435,0.4, 0.25>	
R1	<0.305,-, ->	<0.305,-, ->	<0.5,-, ->	<0.05,-, ->	<0.525,-, ->	<1,-,->	<0.1525,-, ->	
R2	<0.87,-,->	<0.87,-,->	<1,-,->	<0. 01425,-, ->	<1,-,->	<0.285,-,->	<0.435,-,->	
C1	**<0.5,0.5,->**	**<0.5,0.5,->**	**<0.5,0.5,->**	–	<0.25,-,->	–	**<0.5,0.5,->**	
		<0.5,0.5,->	**<0.5,0.5,->**		**<0.5,0.5,->**			
C2	**<1,1,->**	**<1,1,->**	**<1,1,->**	–	**<1,1,->**	–	**<0.5,-,->**	
C3	<0.35,-, ->	<0.35,-, ->	**<1,1,->**	<0.0475,-,->	**<1,-,->**	<0.175,-,->	<0.175,-, ->	
C4	–	–	–	<0.05,-, ->	<0.05,-, ->	<1,-,->	–	
						<0.05,-,->		
N4	–	–	–	**<0.05,-,->**	**<0.05,-,->**	**<1,-,->**	–	
Risk ≅ damage × probability (10^3(K) $ in one year period)	11.9997	7.9800552	11.28465	0.61785	10.245538625	3.158721	4.465161	Total risk: 49.75167583

Note: Bold vectors are direct impacts in each attack path

Vulnerabilities	Security controls
Chunked code buffer overflow	Upgrading the application with the new version
Oracle TNS listen buffer overflow	Buying another vendor patch products
Unauthorized remote login to database with root privilege	Using secure sockets layer (SSL) communication
Unauthorized remote to user privilege login	Deploying intrusion detection and prevention system
Unauthorized remote to user privilege login	Deploying authentication servers with more hard security features
Unauthorized user to root privilege login	Deploying firewalls
Unauthorized remote to user login to internal computers	
Remote DOS through FTP	Access controls on internal computers
Setup processing viruses through network	Setting up anti-viruses and keeping up with the upgrades
Copying products' analysis plans	Using cryptography techniques
SQL injection	Double authentication for access permissions
DOS through SQL	Using extra stored procedures in DB
	Input validation techniques in Web applications

Table VI. Security controls related to vulnerabilities

Descriptions/ indexes	Security controls (c) 1.1	1.2	2.1	2.2	2.3	2.4	3.1	4.1	5.1	5.2	6.1	6.2
Threats (t)												
1	0.99	0.8	0	0.6	0	0	0	0	0	0	0	0
2	0.99	0.8	0	0.6	0	0	0	0	0	0	0	0
3	0	0	0.6	0.8	0.75	0.9	0	0	0	0	0	0
4	0	0	0.7	0.9	0.85	0.9	0	0	0	0	0	0
5	0	0	0.6	0.8	0.99	0.9	0	0	0	0	0	0
6	0	0	0.6	0.9	0.99	0.7	0	0	0	0	0	0
7	0	0	0	0	0.6	0	0.9	0	0	0	0	0
8	0	0	0	0	0	0	0.5	0.99	0	0	0	0
9	0	0	0	0	0	0	0.5	0.99	0	0	0	0
10	0	0	0	0	0	0	0.5	0	0.99	0.8	0	0
11	0.7	0.7	0.8	0.7	0	0	0	0	0	0	0.99	0.8
12	0.99	0.8	0	0.6	0	0	0	0	0	0	0	0
Cost($)	20	80	200	4,000	3,000	1,400	50	93	2,000	500	60	40

Table VII. Security controls preventive power against threats and implementation cost

$*7,000* for budget, which its chosen controls mitigated *43.2819* amounts of risk and in the next row with $*10,000* for budget, there is only *0.0111* increases in the mitigated risk amount. It means, by considering $*2,600* extra spent money, the mitigated risk will just have a slight change.

5.2 A real-scale evaluation

To verify the soundness and applicability of the proposed model, it was implemented in an organization with 12 servers and more than 1,000 internal user stations. This organization utilizes information systems through three main processes: education and research (BP1), staff recruitment and accounting (BP2) and organizational portal and

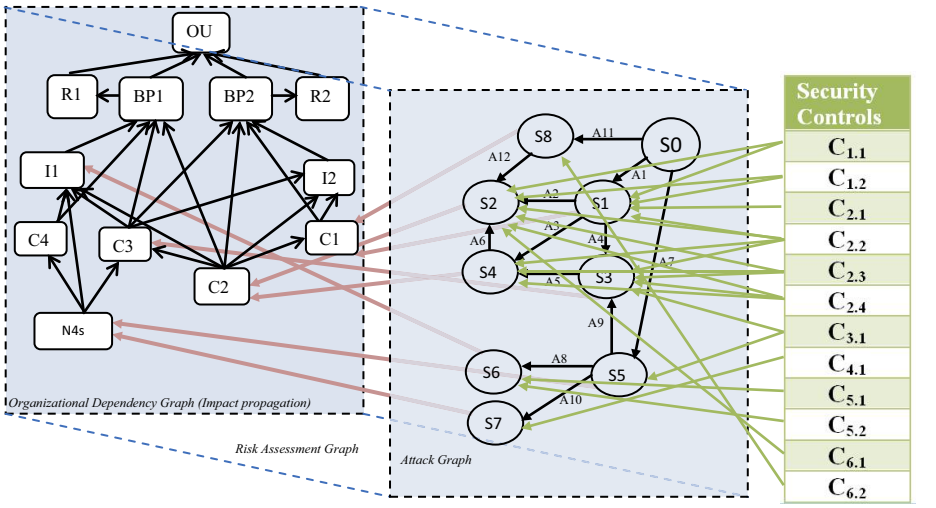

Figure 8.
Mapping controls to attack steps

Budget ($) [used amount]	Our proposed approach optimal security control portfolio	Mitigated risk
100 [70]	1.1, 3.1	18.4618
200 [163]	1.1, 3.1, 4.1	19.6854
300 [270]	1.1, 2.1, 3.1	32.4406
400 [363]	1.1, 2.1, 3.1, 4.1	33.6642
500 [483]	1.1, 1.2, 2.1, 3.1, 4.1, 6.2	33.9310
700 [543]	1.1, 1.2, 2.1, 3.1, 4.1, 6.1, 6.2	33.9409
1,000 [983]	1.1, 1.2, 2.1, 3.1, 4.1, 5.2, 6.2	35.0391
2,000 [1943]	1.1, 1.2, 2.1, 2.4, 3.1, 4.1, 6.1, 6.2	40.5372
3,000 [2443]	1.1, 1.2, 2.1, 2.4, 3.1, 4.1, 5.2, 6.1, 6.2	41.6454
5,000 [4443]	1.1, 1.2, 2.1, 2.4, 3.1, 4.1, 5.1, 5.2, 6.1, 6.2	41.9196
7,000 [6943]	1.1, 1.2, 2.1, 2.3, 2.4, 3.1, 4.1, 5.1, 6.1, 6.2	43.2819
10,000 [9543]	1.1, 1.2, 2.1, 2.2, 2.3, 3.1, 4.1, 5.1, 6.1, 6.2	43.2930
20,000 [11443]	1.1, 1.2, 2.1, 2.2, 2.3, 2.4, 3.1, 4.1, 5.1, 5.2, 6.1, 6.2	43.3624

Table VIII.
Optimal subset of security controls per different budgets

electronic post service management (BP3). Separated information systems, including Web and database servers, were used through these business processes, as presented in Figure 9. Detailed information about dependency types and weights was asked to construct the organization asset dependency graph. Furthermore, the most experienced threats which are reported by Verizon (2013) and top 20 critical security controls that are advised by SANS (2013) were used as initial threat and control list for RM. Risk assessment input data such as assets value, vulnerabilities and related threats probability and severity of occurrence were estimated using experts experience and threat reports in an organization. After assessing the related vulnerabilities for technical assets and designing an attack graph, risk of compromising any vulnerability was calculated using RAG, although graphs and detail information used for risk assessment and mitigation are excluded.

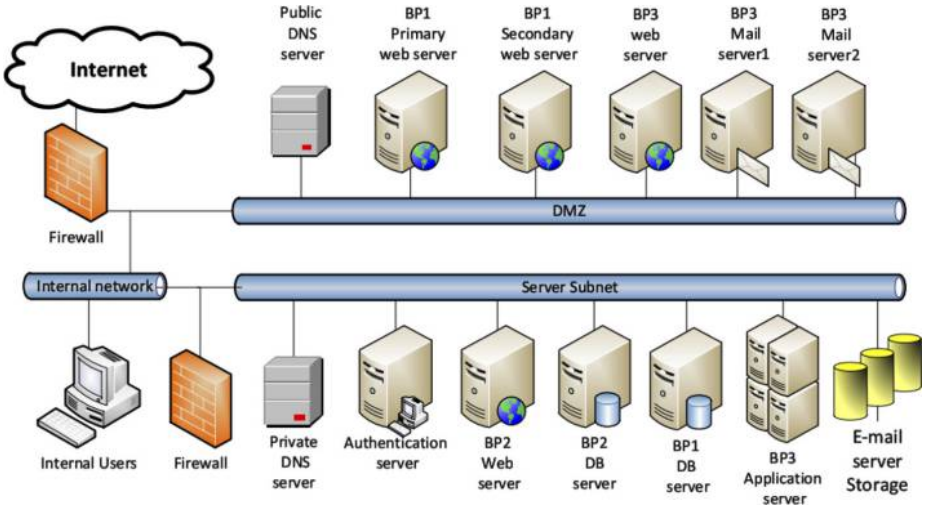

Figure 9.
Case study organization computer network scheme

Table IX indicates the difference between risk amounts for a subset of probable attacks. The risk was calculated in two cases of considering and not considering risk diffusion among interdependent assets, as presented in the proposed model.

As discussed, the assessed risk amount up to this level of model implementation is going to be used as one of the most important indicators in control selection. As can be seen in Table IX, considering dependent asset structure in risk assessment had led to more accurate risk amounts in most cases. For *bruteforce/using stolen credentials* and *sniffing* attacks, the resulted risks are the same in both cases. These attacks, impact the targeted asset confidentiality. Since the dependency matrix among targeted asset and dependent assets has "-" value for confidentiality impact diffusion in all criteria, the risk of those attacks did not diffused to other dependent assets.

To select the optimal subset of security controls, a table similar to Table VII, inspiring by the one shown in Figure 10, is used to measure the effectiveness of 20 security controls in SANS (2013). Moreover, the cost of implementation for these controls in the case study organization is estimated by security experts. After running

		Security Controls																			
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Threat Actions	Tampering	•		•				•		•											
	Spyware		•	•		•							•								
	Backdoor		•	•		•	•				•	•	•	•							
	Export data		•	•		•					•		•	•				•		•	
	Use of stolen creds							•		•	•		•								
	Capture stored data		•	•		•							•			•		•		•	
	Phishing		•	•		•				•			•	•							•
	C2		•	•		•	•				•	•	•	•							
	Downloader		•	•		•							•	•							
	Brute force		■				•	•		•	•		•	•	•	•	•				

Source: Verizon (2013)

Figure 10.
Verizon furnished threat-control matrix

the proposed algorithm, using this information, optimal subset of security controls were obtained per four different budgets, as presented in Table X (Figures 10, 11).

The following details are the examples of the algorithm output that are shown in tabular form in Figure 11. Controls number 2, 3 and 12 that are about *software whitelisting*, *secure configuration of hardware and software* and *administrative privilege control,* respectively, are chosen when available budget is set to $10K. These controls could mitigate around per cent40 (65.4284) of total residual risk (162.1154) by trying to prevent the impact of attacks such as *back door*, *c2*, *phishing*, *tampering* and *brut force*. In the second case, by spending double the amount of money ($18.3K) and implementing extra controls like *vulnerability assessment* (Control 4), *malware defense* (Control 5) and *secure network configuration* (Control 10), almost per cent70 risk mitigation is undertaken.

Regardless of current implementation state of security controls in organizations, decision making should be about all controls' implementation. In better words, at the start point of each decision-making period (e.g. each year), decisions could be made for having currently implemented controls, eliminating a subset of last year controls portfolio or adding new controls to new year portfolio with respect to the allocated budget.

Compared to other RM models that prioritize high-level risks and try to mitigate them step-by-step using the entire budget, the proposed model provides a balance between mitigated risk and used amount of budget. For example, in this case study, *tampering* has the second rank in risk amounts which necessitates implementing a control like *inventory of authorized and unauthorized devices* (Control 1) to mitigate its risk in initial steps. However, the proposed model does not choose this control in the first three cases in Table X. But, it tries to choose controls that cover more risks like *secure configuration of hardware and software* (Control 3).

6. Conclusion

Despite many frameworks and methodologies existing in information security management, decision making still remains confusing and complicated in this area. Security managers are faced with control selection obstacles in complex and dense organizational structures with many units and business processes. In this paper, using a graph-based risk assessment model, the decision making about information security control selection in the risk mitigation phase is improved. At first, features for security controls were defined; then, considering security implementation budget as a limit, and following a knapsack-based model for control selection, the optimal action plan portfolio for risk mitigation was resulted. The proposed model covers risk assessment and risk mitigation as main RM procedures. It also ensures security managers that if a control is chosen for implementation, its effectiveness is not only about its prevention power on

Budget ($K) [used amount]	security control portfolio	Mitigated risk
10[9.85]	2,3,12	65.4284
20[18.3]	2,3,4,5,10,12	112.9183
30[29.51]	2,3,4,5,6,7,9,10,12,13	145.2511
60[58.93]	1,2,3,4,5,6,8,9,10,11,12,13,14,15,16,17,18,19,20	158.9305
		Total risk = 162.1154

Figure 11.
Optimal subsets of controls per different budgets in case study organization

the host asset, it is also about its effectiveness for securing other dependent assets to that host asset. To make a better illustration, a comprehensive example was presented to show the application of the proposed approach. Moreover, results for a real-scale application were discussed with the objective of proposed model validation.

The most significant limitation for the proposed control selection model's utilization is about control effectiveness estimation. Many organizations that have limited experience in security management are forced to trust other reports and simulation results. However, this limitation is because the nature of risk assessment and its ambiguities faced security analyzers with no choice but developing and sharing their experiments more and more.

Notes

1. In this model, we focused on three major aspects in information security: "Confidentiality, Integrity and Availability". Attackers target these aspects to compromise as direct or indirect goal in an attack. More information can be referred to (Avizienis *et al.*, 2004).
2. Return on investment.
3. NVD – National Vulnerability Database provided a list of vulnerabilities under NIST organization supervision; more information can be referred to http://nvd.nist.gov/
4. CVE – Common Vulnerabilities and Exposures as a standard for vulnerability coding and their severity of exploitation, more information can be referred to http://cve.mitre.org/
5. CVSS – Common Vulnerability Scoring system.
6. Readers who are interested in more details may refer to (Breu *et al.*, 2008).
7. http://nvd.nist.gov/

References

Albert, C. and Dorofee, A. (2003), "Introduction to the OCTAVE approach", Carnegie Mellon Software Engineering Institute, pp. 4-16.

Alpcan, T. and Bambos, N. (2009), "Modeling dependencies in security risk management", *Fourth International Conference on Risks and Security of Internet and Systems (CRiSIS)*, *IEEE, Toulouse*.

Avizienis, A., Laprie, J.C., Randell, B. and Landwehr, C. (2004), "Basic concepts and taxonomy of dependable and secure computing", *IEEE Transactions on Dependable and Secure Computing*, Vol. 1 No. 1, pp. 11-33.

Boehmer, W. (2008), "Appraisal of the effectiveness and efficiency of an information security management system based on ISO 27001", *2nd International Conference on Emerging Security Information Systems and Technologies (SECURWARE'08)*, *IEEE, Cap Esterel.*

Breu, R., Innerhofer-Oberperfle, F. and Yautsiukhin, A. (2008), "Quantitative assessment of enterprise security system", *Proceedings of the 3rd International Conference on Availability, Reliability and Security*, *IEEE, Barcelona*.

BritishStandard (2006), "BS7799 -3:2006, information security management systems -Part 3: guidelines for information security risk management".

Demetz, L. and Bachlechner, D. (2013), "To invest or not to invest? Assessing the economic viability of a policy and security configuration management tool", *The Economics of Information Security and Privacy*, Springer Berlin Heidelberg, pp. 25-47.

Dewri, R., Poolsappasit, N., Ray, I. and Whitley, D. (2007), "Optimal security hardening using multi-objective optimization on attack tree models of networks", *Proceedings of the 14th ACM Conference on Computer and Communications Security, ACM, New York, NY*.

Dewri, R., Ray, I., Poolsappasit, N. and Whitley, D. (2012), "Optimal security hardening on attack tree models of networks: a cost-benefit analysis", *International Journal of Information Security*, Vol. 11 No. 3, pp. 167-188.

Eom, J.-H., Park, S.-H., Kim, T.-K. and Chung, T.-M. (2005), "Two-dimensional quantitative asset analysis method based on business process-oriented asset evaluation", *Journal of Information Processing Systems*, Vol. 1 No. 1, pp. 79-85.

Hagen, J.M., Albrechtsen, E. and Hovden, J. (2008), "Implementation and effectiveness of organizational information security measures", *Information Management & Computer Security*, Vol. 16 No. 4, pp. 377-397.

Innerhofer-Oberperfle, F. and Breu, R. (2006), "Using an enterprise architecture for IT risk management", *Proceedings of ISSA-06*.

ISO (2008), "Information security risk management, international standard organization", *ISO/IEC* 27005.

ISO (1998), "Information technology -guidelines for the management of ITSecurity – part 3: techniques for the management of IT Security", ISO/lEC TR 13335-3.

Jahnke, M., Thul, C. and Martini, P. (2007), "Graph based metrics for intrusion response measures in computer networks", *Proceedings of Local Computer Networks*, IEEE, Dublin.

Liu, H.-L. and Zhu, Y.-J. (2009), "Measuring effectiveness of information security management", *International Symposium on Computer Network and Multimedia Technology, CNMT*, IEEE, Wuhan.

Mell, P., Scarfone, K. and Romanosky, S. (2007), "A complete guide to the common vulnerability scoring system version 2.0", FIRST-Forum of Incident Response and Security Teams.

MFPA (2012), "Magerit version 3 (Spanish): methodology of risk analysis and management of information systems", Ministry of Finance and Public Administration.

Moody, D.L. and Walsh, P. (1999), "Measuring the value of information-an asset valuation approach", ECIS.

Mounzer, J., Alpcan, T. and Bambos, N. (2010a), "Integrated security risk management for IT-intensive organizations", *6th International Conference on Information Assurance and Security (IAS)*, IEEE, Atlanta, GA.

Mounzer, J., Tansu, A. and Bambos, N. (2010b), "Dynamic control and mitigation of interdependent IT security risk", *International Conference on Communications (ICC), IEEE*, Cape Town.

Neubauer, T., Ekelhart, A. and Fenz, S. (2008), "Interactive selection of ISO 27001 controls under multiple objectives", *Proceedings of The IFTP – Tc 11 23rd International Information Security Conference*, *Springer, Milano*.

Paintsil, E. (2012), "Taxonomy of security risk assessment approaches for researchers", *4th International Conference on Computational Aspects of Social Networks (CASoN)*, *IEEE*.

Poolsappasit, N. (2010), "Towards an efficient vulnerability analysis methodology for better security risk management", PhD Dissertation, Colorado State University.

Poore, R.S. (2000), "Valuing information assets for security risk management", *Auerbach Publications*, Vol. 9 No. 4, pp. 1-7.

Rakes, T.R., Deane, J.K. and Rees, L.P. (2012), "IT security planning under uncertainty for high-impact events", *Omega: International Journal of Management Science*, pp. 79-88.

Rees, L.P., Deane, J.K., Rakes, T.R. and Baker, W.H. (2011), "Decision support for Cybersecurity risk planning", *Decision Support Systems*, Vol. 51 No. 3, pp. 493-505.

SANS (2013), "Top 20 critical security controls".

Sawik, T. (2013), "Selection of optimal countermeasure portfolio in IT security planning", *Decision Support Systems*, Vol. 55 No. 1, pp. 156-164.

Sawilla, R.E. and Ou, X. (2008), 'Identifying critical attack assets in dependency attack graphs', *13th European Symposium on Research in Computer Security*, Springer Berlin Heidelberg.

Shahpasand, M. and Hashemi, G.A. (2013), "Optimum countermeasure portfolio selection: a knapsack approach", *Emerging Trends in ICT Security – Chapter 19*.

Sheyner, O. (2004), *Scenario Graphs and Attack Graphs*, University of Wisconsin.

Soldal, LM, Solhaug, B. and Stolen, K. (2011), *Model-Driven Risk Analysis: The CORAS Approach*, Springer.

Stoneburner, G., Goguen, A. and Feringa, A. (2002), *Risk Management Guide For Information Technology Systems*, NIST Special Publication.

Torres, J.M., Sarrieg, J.M., Santos, J. and Serrano, N. (2006), "Managing information systems security: critical success factors and indicators to measure effectiveness", *Information Security*, Springer Berlin Heidelberg, pp. 530-545.

Verizon (2013), "Data breach investigations report", available at: www.verizonenterprise.com/DBIR/2013

Viduto, V., Maple, C., Huang, W. and López-Peréz, D. (2012), "A novel risk assessment and optimisation model for a multi-objective network security countermeasure selection problem", *Decision Support Systems*, Vol. 53 No. 3, pp. 599-610.

Yazar, Z. (2002), "A qualitative risk analysis and management tool – CRAMM", SANS InfoSec Reading Room White Paper.

Zhang, Z., Wang, S. and Kadobayashi, Y. (2013), "Exploring attack graph for cost-benefit security hardening: a probabilistic approach", *Computer & Security*, Vol. 23, pp. 158-169.

Further reading

Asghari, M. and Shariari, H. (2010), "Threat propagation modeling based on the relationship of assets and vulnerabilities for security risk analysis", *16th Annual International Conference of Computer Society of Iran*, Computer Society of Iran, Tehran-Iran (In persian).

Bistarelli, S., Fioravanti, F. and Peretti, P. (2007), "Using cp-nets as a guide for countermeasure selection", *ACM Symposium on Applied Computing*, Seoul.

Blakley, B., McDermott, E. and Geer, D. (2001), "Information security is information risk management', *Proceedings of the workshop on New security paradigms*, ACM, NY, NY, USA.

Homer, J., Ou, X. and Schmidt, D. (2009), "A sound and practical approach to quantifying security risk in enterprise networks", KS State University Technical Report.

Homer, J., Varikut, A., Ou, X. and McQueen, M.A. (2008), "Improving attack graph visualization through data reduction and attack grouping", *Visualization for Computer Security*, Springer Berlin Heidelberg.

Ingols, K., Lippmann, R. and Piwowarski, K. (2006), "Practical attack graph generation for network defense", *ACSAC'06 22nd Annual Conference on Computer Security Applications, IEEE, Miami Beach, FL*.

ISO (2013), "Security techniques – information security management systems", ISO/IEC 27001, International Organization for Standardization and International Electrotechnical Commission.

Lv, H. (2009), "Research on network risk assessment based on attack probability", *Proceedings of 2nd International Workshop on Computer Science and Engineering*, Qingdao.

Marinos, L. (2013), "ENISA threat landscape 2013", ENISA.

Noel, S., Jacobs, M., Kalapa, P. and Jajodia, S. (2005), "Multiple coordinated views for network attack graphs", *IEEE Workshop on Visualization for Computer Security*, IEEE.

Rong, A., Figueira, J.R. and Pato, M.V. (2011), "A two state reduction based dynamic programming algorithm for the bi-objective 0-1 knapsack problem", *Computers & Mathematics with Applications*, Vol. 62 No. 8, pp. 2913-2930.

RTO (NATO) (2008), "Analysis, RTO-TR-IST-049-PRE-RELEASE: improving common security risk', research and technology organisation (NATO)", BP 25, F-92201 Neuilly-sur-Seine Cedex.

Sheyner, O., Haines, J., Jha, S., Lippmann, R. and Wing, J.M. (2002), "Automated generation and analysis of attack graphs", *Proceedings of the IEEE Symposium on Security and Privacy*, Oakland, CA.

Vorster, A. and Les, L. (2005), "A framework for comparing different information security risk analysis methodologies", *Annual Research Conference of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries*, South African Institute for Computer Scientists and Information Technologists.

Wang, L., Islam, T., Long, T., Singhal, A. and Jajodia, S. (2008), "An attack graph-based probabilistic security metric", *Data and Applications Security XXII*, Springer Berlin Heidelberg, pp. 283-296.

Williams, L., Lippmann, R. and Ingols, K. (2007), "An interactive attack graph cascade and reachability display", *VizSEC 2007*, Springer Berlin Heidelberg.

Corresponding author
Maryam Shahpasand can be contacted at: m.shahpasand7@gmail.com