International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:7, No:8, 2013

Effective Methodology for Security Risk Assessment of Computer Systems

Daniel F. García and Adrián Fernández

***Abstract*—**Today, computer systems are more and more complex and support growing security risks. The security managers need to find effective security risk assessment methodologies that allow modeling well the increasing complexity of current computer systems but also maintaining low the complexity of the assessment procedure. This paper provides a brief analysis of common security risk assessment methodologies leading to the selection of a proper methodology to fulfill these requirements. Then, a detailed analysis of the most effective methodology is accomplished, presenting numerical examples to demonstrate how easy it is to use.

***Keywords*—**Computer security, qualitative and quantitative methods, risk assessment methodologies, security risk assessment.

I. Introduction

THE evaluation of security risks in computer systems is increasingly important because of the steady growth of security threats. This growth is because the systems are increasingly interconnected and exchange a greater amount of information. Generally, the security risk evaluation methods are classified as qualitative and quantitative.

The qualitative methods use a scale of qualitative values (e.g. Low, Medium, High) to represent the value of the assets and the impacts and risks suffered by them.

The quantitative methods use a measure of value, e.g. Euros, to represent the value of the assets of a computer system and also the levels of impact and risk supported by the assets.

The main advantage of the quantitative methods is that they can provide approximate estimations of the impact provoked by a threat on an asset in the form of a Single Loss Expectancy (SLE) and estimations of the risk in the form of Annual Loss Expectancy (ALE).

There are risk evaluation methodologies that only use a qualitative method and others than only use a quantitative method. The most interesting methodologies integrate two methods, one qualitative and other quantitative, and therefore, they allow the development of a first preliminary analysis to determine the main risks and a second detailed analysis, probably focused in the most important risks. But, it is highly desirable that both methods are based in similar models of the computer system.

In this paper the methods used in common methodologies are briefly analyzed, and later, the methods used in the most effective methodology are analyzed deeply.

D. F. García is with the University of Oviedo, Department of Informatics, 33204 Gijón (Asturias), Spain (phone: 34-985-182066; fax: 34-985-181986; e-mail: dfgarcia@uniovi.es).

A. Fernández is with the University of Oviedo, Department of Informatics, 33204 Gijón (Asturias), Spain. (e-mail: uo170656@uniovi.es).

II. Related Work

Many methods have been proposed in the literature to evaluate the risks suffered by a computer system and they have been compared, directly [1] and using frameworks [2].

There are methods that are very generic, in fact they are guidelines for managing information security risks in an organization. A typical example of these guidelines is the standard ISO/IEC 27005 [3]. Other standards are more specific, providing the typical sequence of activities required for risk assessment and risk mitigation, but including also a specific method for determining the risks. An example is the Risk Management Guide for IT Systems provided by NIST [4] that is currently under revision [5].

In the analysis of currently available methods for evaluation of security risks, two main categories should be considered:

The many methods proposed by a myriad of researchers that can be used for specific security problems.

The few methods developed by national or international institutions that are widely used and they are often supported by computer tools.

A. Methods Proposed by Researchers

Many researchers have proposed information security risk analysis methodologies. Some methodologies are simple and very easy to use, like those using matrices to correlate the elements of risk analysis [6]. Other researchers have also used very simple models and small tables to manage Information Technology security risks [7]. Other methodologies, like ISRAM [8], fill tables with values obtained from multiple interviews and use the values to estimate the risk.

Other modern methods are even simpler, establishing general procedures and using elemental metrics to develop a security risk assessment [9], [10]. The authors argue that a truly practical method should be fairly simple.

Other approach used to develop security risk assessment methods consists in adapting risk management methods from other scientific disciplines. Then, some researchers have developed useful methods adapting software risk management techniques [11]. Other researchers have proposed the application of techniques used for accident risk assessment in industrial plants, like Probabilistic Risk Assessment (PRA), to the information security risk assessment in computer systems [12]. The similarities are really surprising allowing the utilization of a methodology in different application domains.

Recently, sophisticated methods for risk assessment based

on neural networks, fuzzy sets and other technologies based on soft computing techniques are appearing [13]-[15].

B. Methods Proposed by Institutions & Companies

In this category, methods as NIST 800-30, OCTAVE, Mehari, Microsoft's Security Management Guide and Magerit can be considered.

The methodology proposed by NIST is qualitative using 5 descriptors (very low, low, moderate, high, very high) to characterize the impact and also the same 5 descriptors to characterize the likelihood of the impact. It also provides a table for translating these descriptors in numbers in a scale from 0 to 10 to carry out a semi-quantitative analysis. This method provides general rules and requirements for system characterization, but it does not provide a specific model to characterize the assets and their interrelations.

The OCTAVE [16] (Operationally Critical Threat, Asset and Vulnerability Evaluation) methodology was developed by the Software Engineering Institute of Carnegie Mellon University. This methodology is quite generic, like ISO/IEC 27001/27005 and the analysis method is qualitative, trying to find the most relevant risks to treat them first. In fact, it is mainly used as a prioritization tool for the risks supported by an organization.

Mehari is a methodology proposed by the Club de la Sécurité de l'Information Français (CLUSIF). The risk analysis method [17] is qualitative, and the risk (seriousness in Mehari terminology) is represented in a scale from 1 to 4. In Mehari, the classification of assets [18] is done in three domains linked between them. An Excel book with multiple spreadsheets provides support for this classification and the posterior risk analysis process. Nevertheless, there is not a clear model that represents the interrelations between the domains. This could be understood because Mehari works mainly with groups or types of assets.

Microsoft's Security Risk Management Methodology [19] follows a hybrid approach. Firstly, a qualitative method is used to quickly prioritize the entire list of security risks. Then, the most important risks identified in the first phase are evaluated in more detail using a quantitative method.

Basically, all the methods reviewed consider each asset independently, evaluating the impact and likelihood of threats over the asset. Essentially, the model is a list of assets and there is a lack of a clear definition of the possible interrelations between the assets and how these interrelations affect to the risk supported by any of the assets of the computer system.

Finally, Magerit [20] is a methodology promoted by the Spanish Ministry for Public Administrations. It must be used by Spanish public administrations, but it can also be used by public and private corporations.

The assessment methods used by this methodology allow the characterization of dependencies between assets. In the qualitative method, the dependencies are Boolean (exist or not exist), but in the quantitative method, the dependencies are a real number between 0.0 (no dependency) and 1.0 (total dependency).

This methodology allows the representation of the relations that always exist between the assets of a computer system much better than the other methodologies analyzed in this research work.

The rest of this paper presents the essence of the two security risk assessment methods supported by Magerit, providing numerical examples to illustrate their utilization. The main objective is to show the real power and simplicity of this little-known methodology and to bring awareness between security professionals.

III. Qualitative Method

The aim of the qualitative method is to provide a qualitative comparison of the risks suffered by the assets of a computer system in a predefined value scale. Therefore, a scale of symbolic value levels is defined by (1).

$$V = \{ ..., v_0, v_1, ..., v_i, ... \} \quad (1)$$

Each asset must receive a value of this scale in each dimension of security: confidentiality, Integrity and Availability (CIA).

A. Dependencies between the Assets

But the assets are not independent entities. Generally, there are dependencies between the assets.

This qualitative method only considers the presence of a dependency and not the level of the dependency. If an asset A depends on other asset B, (2) express the dependency.

$$A \rightarrow B \quad (2)$$

Of course, the dependency can be transitive, when an asset A depends on B and B depends on C, which can be expressed as: $(A \rightarrow B) \Lambda (B \rightarrow C)$. In this case, A depends on B directly and A depends on C indirectly though B.

The dependencies can be more complex. A typical example is (3) when A depends on B_1 and B_2 and B_i depend on C.

$$(A \rightarrow B_1) \Lambda (A \rightarrow B_2) \Lambda (B_1 \rightarrow C) \Lambda (B_2 \rightarrow C) \quad (3)$$

These dependencies can be represented by a graph. Fig. 1 shows two examples of this type of graphs.

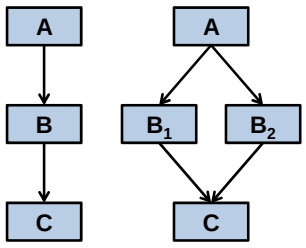

Fig. 1 Dependency graphs between assets

The set of assets that depend on B, directly or indirectly, is denominated Superior of B, SUP (B). These assets are above B in the graph. Equation (4) represents this set.

$$SUP(B) = \{ A_i, A_i \rightarrow B \} \quad (4)$$

The concept of dependency allows the definition of the accumulated value over an asset.

B. Accumulated Value over an Asset

The accumulated value over an asset B is defined as the highest value among B and the assets A_i included in the set SUP(B). Equation (5) represents this value.

$$Acc\_Val(B) = MAX [Val(B), max_i\{ Val(A_i) \}] \quad (5)$$

C. Degradation of the Value of an Asset

When an asset is victim of a threat, it loses part of its value. A subjective percentage of degradation must be estimated to characterize the loose of value. Then, the degradation will be a value between 0.0 (0% degradation) and 1.0 (100% degradation).

D. Accumulated Impact of a Threat on an Asset

The accumulated impact of a threat on an asset is the loose of accumulated value of the asset. If an asset has an accumulated value of v_x and it is degraded by a proportion d, (6) provides an estimation of the value of the impact.

$$Impact\ i = v_{ROUND(x \cdot d)} \quad (6)$$

when the impact is reduced to v_0, it can be considered as negligible.

E. Deflected Impact of a Threat on an Asset

If an asset A depends on other asset B, any threat to B will also affect A. Fig. 2 illustrate this situation.

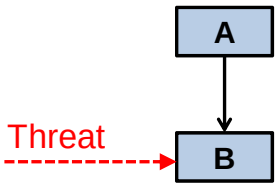

Fig. 2 Deflected impact of a threat on an asset

If B suffers a degradation d, A will suffer the same degradation loosing value. If the asset A has a value v_x the impact will be calculated by using (7):

$$defected\ impact\ di = v_{ROUND(x \cdot d)} \quad (7)$$

F. Frequency of Threats

In this qualitative method the frequency of threats must be characterized by a scale of symbolic values, as defined by (8).

$$F = \{ ..., f_0, f_1, ..., f_j, \ldots \} \quad (8)$$

The series of frequency values must verify the following properties:

There is a total order: $f_j < f_{j+1}$.

There is an element, f_0, which represents the "negligible frequency".

There is an element, f_n, that represent the "normal frequency". In an annual risk analysis, the value f_n refers to "once a year".

Informally, we say that a threat has "j frequency points" to indicate that its frequency is f_j.

G. Risks

The risks values are represented in the same scale used to represent the value of the assets. The risk is a function, ***R***, of the impact and the frequency defined by (9).

$$Risk = \boldsymbol{R}(impact, frequency) \quad (9)$$

The function ***R*** must verify the following requirements:

1. It must grow with the impact (10).

$$\forall\ fj\ \ R(vi, fj) < R(vi+1, fj) \quad (10)$$

2. It must grow with the frequency (11).

$$\forall\ vi\ \ R(vi, fj) < R(vi, fj+1) \quad (11)$$

3. It must generate a negligible risk for a negligible impact and a normal frequency (12).

$$\boldsymbol{R}(v_0, f_n) = v_0 \quad (12)$$

A very simple function that fulfills these properties is defined by (13).

$$\boldsymbol{R}(v_i, f_j) = v_{i+j-n} \quad (13)$$

Any risk that takes a value v_0 or less will be considered negligible.

Two different types of risk can be calculated as a function of the value considered for the assets:

The accumulated risk is calculated with the accumulated impact over the asset.

The deflected risk is calculated with the deflected impact over the asset.

H. Security Controls

A set of security controls is deployed against a threat. The controls have efficiency, e, reducing the degradation of the asset provoked by the threat. The efficiency e is a value between 0.0 (no protection) and 1.0 (full protection). Furthermore, the efficiency e can be decomposed in an efficiency against the impact, e^i, and an efficiency against the frequency, e^f.

I. Residual Degradation

The effect of security controls is reducing the degradation suffered by an asset. If the asset, without protection, could suffer degradation d, thanks to controls, the degradation is reduced to a residual value rd, calculated using (14).

$$rd = d \times (1-e^i) \quad (14)$$

where e^i is an estimation of the efficiency of controls to reduce the degradation of the asset, that is, limiting the impact on the asset. The values of e^i are in the following range:

$e^i = 0.0$, then: rd = d (useless controls)

$e^i = 1.0$, then: rd = 0 (perfect controls)

J. Residual Impact

When an asset is protected by security controls suffers a residual impact, which can be calculated just like the impact, but using the residual degradation, calculated by (15).

$$residual\_impact = V_{ROUND(x \cdot rd)} \quad (15)$$

A set of perfect security controls reduces the impact to a negligible value v_0. If the controls are not enough, the impact will remain noticeably.

K. Residual Frequency

The second effect of a security control is to reduce how often a threat gets to attack an asset successfully exploiting vulnerability. Similarly to the case of impact, the frequency of the threat to the asset is reduced to a residual value. If the frequency was f_j, now with controls, the residual frequency is defined by (16).

$$residual\_frequency = f_k \text{ where } k = ROUND(\, j \cdot (1-e^f) \,) \quad (16)$$

where e^f is the efficiency of the security controls reducing the frequency of the threat. The value of e^f is in the range:

$e^f = 0.0$, then $f_k = f_j$ (useless controls)

$e^f = 1.0$, then $f_k = f_0$ (perfect controls)

L. Residual Risk

Finally, the residual risk is calculated using (17) which combines the residual impact and the residual frequency using the function R defined previously.

$$residual\ risk = \boldsymbol{R}(residual\ impact, residual\ frequency) \quad (17)$$

In this qualitative method, a relative value has been assigned to each asset selected from a scale defined previously. A value v_0 has been chosen as the boundary between the significant values and those that are negligible.

On this scale of value has been measured both, the value of the asset (basic or accumulated), as the impact of a threat when it occurs, and the risk suffered by the asset.

While the impact measures the potential loss of value, the risk weights that impact with the estimated frequency of occurrence of the threat. The impact is the measure of the cost if the threat occurs once while the risk measures the exposure in a given period of time.

The estimates of residual impact and residual risk incorporate the efficiency of security controls to counteract the threat, either by limiting the impact, either by reducing the frequency.

This qualitative method, prior to use, requires a valuation or estimation of several magnitudes:

Valuation of the assets through a discrete scale of values.

Estimation of the degradation caused by the threats expressed as a percentage.

Estimation of the frequency of occurrence of each threat expressed in a discrete scale of frequencies.

Selection of a set of security controls.

Estimation of the efficiency of the controls, expressed as a percentage.

IV. Qualitative Numerical Example

This example has two assets, A and B. The value of the assets, the impacts and risks suffered will be valued in the scale $V = \{ v_0, v_1, ..., v_i, ..., v_{10} \}$, where v_0 represents a negligible value.

The value of asset A is v_8 and the threat T_A provokes a degradation on A of d(A)=70%.

The value of asset B is v_B (irrelevant in this example) and the threat T_B provokes a degradation of B of d(B)=35%.

The asset A depends on B. Therefore any degradation suffered by B is also directly deflected to A.

The frequency of the threats is represented in the discrete scale $F = \{ f_0, f_1, ..., f_j, ..., f_5 \}$, where f_0 represents a negligible frequency. The normal frequency, f_n, is in this example f_3.

The frequency of T_A is f_2.

The frequency of T_B is f_4.

With these data, the method allows the estimation of impacts (direct and deflected) using (18) and (19).

$$impact = v_{ROUND(8 \times 0.7)} = v_6 \quad (18)$$

$$deflected\ impact = v_{ROUND(8 \times 0.35)} = v_3 \quad (19)$$

Now, the risks (direct and deflected) can be estimated by (20) and (21) combining the impacts with their frequencies using the function $\boldsymbol{R}(v_i,f_j) = v_{i+j-n}$ defined previously.

$$risk = \boldsymbol{R}(v_6,f_2) = v_{6+2-3} = v_5 \quad (20)$$

$$deflected\ risk = \boldsymbol{R}(v_3,f_4) = v_{3+4-3} = v_4 \quad (21)$$

The results of the method for the risk assessment are presented in Fig. 3 in a graphical manner. The value of the asset A, v_8, is represented with a green bar. When the asset A suffers the impact of the threat T_A loses 6 units of value, v_6, and when the asset A suffers the impact of the threat T_B loses 3 units of value, v_3. Therefore, the yellow bars of Fig. 3 represent the part of the green bar that is lost due to the degradation provoked by the threats.

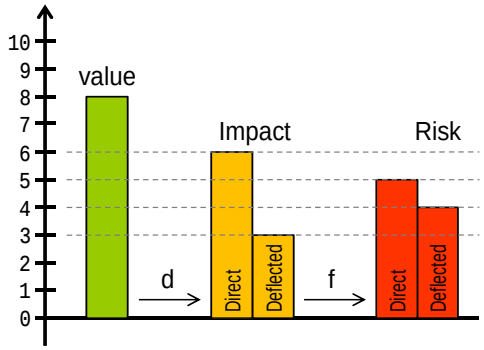

Fig. 3 Visualization of risk assessment results

Then, the frequency f of the threats is used to transform the impact values in risks values. Due to the frequency of the thread T_A is one unit lower than the normal frequency, the impact value is reduced in one unit to generate the risk. On the contrary, as the frequency of the threat T_B is one unit higher than the normal frequency, the deflected impact is increased in one unit to generate the deflected risk. Both risks are represented by red bars in Fig. 3.

In order to reduce the risks, a set of security controls are selected to reduce the impact and the frequency of threats.

The control for T_A has an efficiency against the impact of e^i=0.5 and against the frequency of e^f=0.6.

The control for T_B has an efficiency against the impact of e^i=0.4 and against the frequency of e^f=0.8.

Firstly, the direct residual risk suffered by the asset A as a consequence of the threat T_A is calculated by (22)–(25).

$$\text{residual deg}(A) = d(A) \times (1-e^i) = 0.7 \times (1-0.5) = 0.35 \quad (22)$$

$$\text{residual impact} = v_{ROUND(8 \times 0.35)} = v_3 \quad (23)$$

$$\text{residual frequency} = f_{ROUND(2 \times (1-0.6))} = f_1 \quad (24)$$

$$\text{residual risk} = \boldsymbol{R}(\text{res\_i}, \text{res\_f}) = \boldsymbol{R}(v_3, f_1) = v_{3+1-3} = v_1 \quad (25)$$

Secondly, the residual deflected risk suffered by the asset A as a consequence of the threat T_B is calculated by (26)–(29).

$$\text{residual deg}(B) = d(B) \times (1-e^i) = 0.35 \times (1-0.4) = 0.21 \quad (26)$$

$$\text{residual deflected impact} = v_{ROUND(8 \times 0.21)} = v_2 \quad (27)$$

$$\text{residual deflected frequency} = f_{ROUND(4 \times (1-0.8))} = f_1 \quad (28)$$

$$\text{residual deflected risk} = \boldsymbol{R}(\text{res\_di}, \text{res\_df}) = \boldsymbol{R}(v_2, f_1) = v_{2+1-3} = v_0 \quad (29)$$

V. Quantitative Method

The aim of the quantitative method is to provide an estimation of the risks suffered by the assets expressing the risks in real numeric values (euro, dollar).

The value of any asset in a specific dimension of security (CIA) is a real value higher than zero. A specific value, v_0, is defined as the limit between negligible and relevant values.

A. Dependencies between the Assets

The concepts of dependency between assets defined for the qualitative method are also applied here. But as the quantitative method should be more precise, the concept of dependency is refined. In the qualitative method the dependency between two assets is a binary property. In the quantitative method the dependency is characterized by a coefficient between 0.0 (independent assets) and 1.0 (totally dependent assets). The coefficient is called "degree of dependency".

These dependencies can be represented by a graph. The degree of direct dependency between two assets is represented by a percentage on the arrow that connects the two assets. Fig. 4 represents two examples of this type of graphs.

To calculate the degree of dependency of an asset A from other asset C, the expression (30) is used.

$$\text{degree}(A \rightarrow C) = \sum_i \{\text{degree}(A \rightarrow B_i) \times \text{degree}(B_i \rightarrow C)\} \quad (30)$$

where the sums are carried out as defined by (31).

$$p + q = 1 - (1-p) \times (1-q) \quad (31)$$

The set of assets that depend on B, directly or indirectly, is denominated Superior of B, SUP (B).

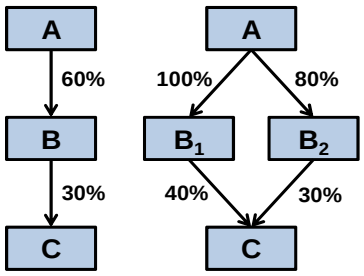

Fig. 4 Dependency graphs between assets

B. Accumulated Value over an Asset

The accumulated value over an asset B is defined by (32) as the addition of the own value of the asset plus the sum of the values of the superior assets, weighted by the degree of dependency.

$$\text{Acc\_Val}(B) = \text{Val}(B) + \sum_i \{\text{Val}(A_i) \times \text{degree}(A_i \rightarrow B)\} \quad (32)$$

C. Degradation of the Value of an Asset

When an asset is victim of a threat, it suffers a degradation that is characterized by a value between 0.0 (0% degradation) and 1.0 (100% degradation).

D. Accumulated Impact of a Threat on an Asset

The accumulated impact of a threat on an asset is the loose

of accumulated value of the asset. If an asset has an accumulated value v and it is degraded by a proportion d, the value of the impact is defined by (33).

$$\text{impact } i = v \times d \tag{33}$$

When the impact is less than v_0 is considered negligible.

E. Deflected Impact of a Threat on an Asset

If an asset A depends on other asset B, any threat to B will also affect A. Fig. 2 illustrated this situation.

If B suffer a degradation d, A will suffer the degradation in the proportion of its dependence on B. If the asset A has a basic value v, the deflected impact is calculated by (34).

$$\text{deflected impact } di = v \times d \times \text{degree}(A \rightarrow B) \tag{34}$$

F. Frequency of Threats

In this quantitative method the frequency of threats is a real value greater than zero. A value, f_0, is established as the "negligible frequency", below which the threat is irrelevant.

G. Risks

The risks is a real value greater than zero that is calculated directly by (35).

$$\text{Risk} = \text{impact} \times \text{frequency} \tag{35}$$

Any risk that takes a value v_0 or less will be considered negligible.

Two different types of risk can be calculated as a function of the value considered for the assets:

The accumulated risk is calculated with the accumulated impact over the asset.

The deflected risk is calculated with the deflected impact over the asset.

H. Security Controls

A set of security controls is deployed against a threat. The controls have an efficiency, e, reducing the degradation of the asset provoked by the threat. The efficiency e is a value between 0.0 (no protection) and 1.0 (full protection). Furthermore, the efficiency e can be decomposed in an efficiency against the impact, e^i, and an efficiency against the frequency, e^f. The decomposition verifies (36).

$$(1 - e) = (1 - e^i) \times (1 - e^f) \tag{36}$$

I. Residual Degradation

The security controls reduce the degradation d suffered by an asset to a residual value rd calculated by (37).

$$rd = d \times (1 - e^i) \tag{37}$$

where e^i is an estimation of the efficiency of controls to reduce the degradation of the asset.

J. Residual Impact

When an asset is protected by security controls suffers a residual impact, which can be calculated by (38), just like the impact, but using the residual degradation.

$$\text{residual\_impact} = v \times rd = v \times d \times (1 - e^i) \tag{38}$$

A set of perfect security controls reduces the impact to a negligible value v_0.

K. Residual Frequency

A security control can also reduce the frequency with which a threat can exploit a vulnerability to attack an asset with success. Then, the frequency of the threat to the asset is reduced to a residual value calculated by (39).

$$\text{residual\_frequency} = \text{frequency} \times (1 - e^f) \tag{39}$$

L. Residual Risk

Finally, the residual risk is calculated by (40) multiplying the residual impact by the residual frequency.

$$\text{residual risk} = \text{residual impact} \times \text{residual frequency} \tag{40}$$

In this quantitative method, a numerical value has been assigned to each asset and a value v_0 has been chosen as the boundary between the significant and negligible values.

The method provides estimations of the impact and risk suffered by the assets. While the impact measures the potential loss of value, the risk weights that impact with the estimated frequency of occurrence of the threat. The impact is the measure of the cost if the threat occurs once while the risk measures the exposure in a given period of time.

The method also calculates estimations of residual impact and residual risk, which incorporate the efficiency of security controls to counteract the threat, either by limiting the impact, either by reducing the frequency.

If the valuation of the asset is economic (the monetary cost derived of its complete loss) the estimated risk is the amount which has to be planned as annual losses. Therefore, the quantitative method allows a direct comparison between the cost of controls and the reduction of losses.

This quantitative method, prior to use, requires a valuation or estimation of several magnitudes:

Valuation of the assets by numerical quantities.

Defining dependencies between assets using percentages.

Estimation of the degradation caused by the threats expressed as a percentage.

Estimation of the frequency of occurrence of each threat expressed as numerical values.

Selection of a set of security controls.

Estimation of the efficiency of the controls, expressed as a percentage.

VI. Quantitative Numerical Example

This example uses the same assets, A and B, of the previous example. The only differences are: the value of the asset A is 10000. The frequency of the threat T_A is 0.5 and the frequency of the threat T_B is 2. The degree of dependency of A from B is of 30%. With these data, the quantitative method estimates the impacts (direct and deflected) using (41) and (42).

$$\text{Impact } i = v_A \times d(A) = 10000 \times 0.7 = 7000 \quad (41)$$

$$\text{Deflected impact } di = v_A \times d(B) \times \text{degree}(A \rightarrow B) = 1000 \times 0.35 \times 0.3 = 1050 \quad (42)$$

Now, the risks (direct and deflected) can be estimated with (43) and (44) multiplying the impacts by the frequencies.

$$\text{risk } r = i \times f(T_A) = 7000 \times 0.5 = 3500 \quad (43)$$

$$\text{deflected risk } dr = di \times f(T_B) = 1050 \times 2 = 2100 \quad (44)$$

In order to reduce the risks, the same set of security controls used in the previous example is selected to reduce the impact and the frequency of threats.

The control for T_A has an efficiency against the impact of e^i=0.5 and against the frequency of e^f=0.6.

The control for T_B has an efficiency against the impact of e^i=0.4 and against the frequency of e^f=0.8.

Firstly, the direct residual risk suffered by the asset A as a consequence of the threat T_A is calculated by (45)–(48).

$$\text{residual degradation } rd(A) = d(A) \times (1-e^i) = 0.7 \times (1-0.5) = 0.35 \quad (45)$$

$$\text{residual impact } ri = v_A \times rd(A) = 10000 \times 0.35 = 3500 \quad (46)$$

$$\text{residual frequency } rf = f(T_A) \times (1-e^f) = 0.5 \times (1-0.6) = 0.2 \quad (47)$$

$$\text{residual risk } rr = ri \times rf = 3500 \times 0.2 = 700 \quad (48)$$

Secondly, the deflected residual risk suffered by the asset A as a consequence of the threat T_B is calculated by (49)–(52).

$$\text{residual degradation } rd(B) = d(B) \times (1-e^i) = 0.35 \times (1-0.4) = 0.21 \quad (49)$$

$$\text{res deflected impact } rdi = v_A \times rd(B) \times \text{degree}(A \rightarrow B) = 10000 \times 0.21 \times 0.3 = 630 \quad (50)$$

$$\text{residual frequency } rf = f(T_B) \times (1-e^f) = 2 \times (1-0.8) = 0.4 \quad (51)$$

$$\text{res deflected risk } rdr = rdi \times rf = 630 \times 0.4 = 252 \quad (52)$$

VII. Conclusion

This paper shows an analysis of most common methodologies used to assess the information security risks supported by computer systems. The results of the analysis show that most of methodologies are too simple and do not consider interrelations between assets explicitly. However, these interrelations always exist in the real computer systems.

The Magerit methodology, illustrated in detail in this paper, represents these interrelations using graphs and provides support for a simple but effective qualitative and quantitative risk analysis considering the interrelations. This paper shows that the Magerit methodology has a great capability to represent complex computer systems and it is very easy to use.

References

[1] A. Syalim, Y. Hori, and K. Sakurai "Comparison of Risk Analysis Methods: Mehari, Magerit, NIST800-30 and Microsoft's Security Management Guide," in Proc. Int. Conf. on Availability, Reliability and Security, Fukuoka, Japan, 2009, pp. 726–731.

[2] A. Vorster, and L. Labuschagne "A Framework for Comparing Different Information Security Risk Analysis Methodologies," in Proc. Annual Research Conf. of the South African Institute of Computer Scientists and Information Technologists on IT Research in Developing Countries, Johannesburg, South Africa, 2005, pp. 95–103.

[3] ISO/IEC, International Standard 27005 on Information Security Risk Management. Geneva, Switzerland: ISO, 2008.

[4] G. Stoneburner, A. Goguen, and A. Feringa, Risk Management Guide for Information Technology Systems. NIST Special Publication 800-30, US Dep. of Commerce, 2002.

[5] NIST, Guide for Conducting Risk Assessments. NIST Special Publication 800-30 Revision 1, US Dep. of Commerce, 2011.

[6] S. Goel, and V. Chen "Information Security Risk Analysis – A Matrix-Based Approach," in Proc. Information Resource Management Association (IRMA) Int. Conf., San Diego, CA, USA, 2005.

[7] D. Gilliam "Managing Information Technology Security Risk," in Proc. Int. Symposium on Software Security, Tokyo, Japan, 2003, LNCS-2004 vol. 3233, pp. 296-317.

[8] B. Karabacaka, and I. Sogukpinar "ISRAM: Information Security Risk Analysis Method," Computers & Security, vol. 24, pp. 147-159, 2005.

[9] A. Asosheh, B. Dehmoubed, and A. Khani "A new quantitative approach for information security risk assessment," in Proc. IEEE Intelligence and Security Informatics Conference, Richardson (Dallas), TX, USA, 2009.

[10] D. V. Bernardo, B. B. Chua, and D. Hoang "Quantitative Security Risk Assessment (SRA) Method: An empirical case study," in Proc. World Congress on Nature & Biologically Inspired Computing, Coimbatore, India, 2009, pp. 972-977.

[11] H. P. In, Y-G. Kim, T. Lee, C.-J. Moon, Y. Jung, and I. Kim "A Security Risk Analysis Model for Information Systems," in Proc. 3rd Asian Simulation Conference on Systems Modeling and Simulation: theory and applications, LNAI vol. 3398, pp. 505-513, 2005.

[12] N. Satoh, and H. Kumamoto "Analysis of Information Security Problem by Probabilistic Risk Assessment," NAUN International Journal of Computers, no. 3, vol. 3, 2009.

[13] X. Long, Q. Yong, L. Qianmu "Information Security Risk Assessment Based On Analytic Hierarchy Process and Fuzzy Comprehensive," in Proc. Int. Conf. on Risk Management & Engineering Management, Beijing, China, 2008, pp. 404-409.

[14] D.-L. Liu, and S.-S. Yang "An Information System Security Risk Assessment Model Based on Fuzzy Analytic Hierarchy Process," in Proc. Int. Conf. on E-Business and Information System Security, Wuhan, China, 2009.

[15] Z. Wang, and H. Zeng "Study on the Risk Assessment Quantitative Method of Information Security," in Proc. 3rd Int. Conf. on Advanced Computer Theory and Engineering, Chengdu, China, 2010, vol. 6, pp. 529-533.

[16] C. Alberts, and A. Dorofee, Managing Information Security Risks: The OCTAVE Approach. Boston, USA: Addison Wesley, 2002.

[17] CLUSIF, MEHARI - Risk Analysis and Treatment Guide, Paris, France: Club de la Sécurité de l'Information Français, 2010.
[18] CLUSIF, MEHARI - Stakes Analysis and Classification Guide, Paris, France: Club de la Sécurité de l'Information Français, 2010.
[19] MICROSOFT, The Security Risk Management Guide, Microsoft Solutions for Security and Compliance and Microsoft Security Center of Excellence, 2006.
[20] F. Lopez, M. A. Amutio, J. Candau, and J.A. Mañas, MAGERIT V2 Book I - The Method. Madrid, Spain: Ministerio de Administraciones Publicas, 2006.

Daniel F. Garcia became a member of **IEEE** in 1994. He was born in Gijón (Spain) in 1959. He obtained the degree of Industrial Engineering (specialized in electronics) by the University of Zaragoza, Spain, in 1983. Later, he obtained the PhD by the University of Oviedo, Spain, in 1988. He joined the University of Oviedo in 1983, where he has developed all his work until today. Since 1994 he leads the area of computer engineering at the University of Oviedo. During the last 20 years, he has developed many projects of basic and applied research, funded by European, national and regional institutions. As result of this research work, he has coauthored 50 articles in journals and more than 130 papers in conferences and workshops.

Adrián Fernández was born in Gijón (Spain) in 1985. He obtained the degree of Computer Engineering by the University of Oviedo, Spain, in 2011. In 2013 he is doing a MSc in Computer Engineering at the University of Oviedo and a MSc in Security of Information Technology and Communications at the Autonomous University of Barcelona. He has also worked from 2011 to today as a software engineer in Talento Corporativo, Spain.