A Proposal for information security risk evaluation framework

Esmat Ali Mohammad Malayeri*, Nasser Modiri,**
Sam Jabbehdari***
*** Islamic Azad- NorthTehran Branch, Tehran Iran,**
esmat.a.m.malayeri@gmail.com
**** Faculty Member**
Islamic Azad- North Tehran Branch, Tehran Iran,
nassermodiri@yahoo.com
***** Faculty Member**
Islamic Azad- North Tehran Branch, Tehran Iran,
s_jabbehdari@iau-tnb.ac.ir

Paper Reference Number:
Name of the Presenter: Esmat Ali Mohammad Malayeri

1-Abstract

Organizations are always facing different threats related to their informational possessions; however, they are extremely dependent to these possessions. Most informational systems are not basically safe and technical solutions are only a small part of the community solutions of comprehensive informational security, so Informational gathering is a necessary task and all organizations should recognize and know the threatening areas which potentially threaten them to do so.

These threatening areas are determined via systematic analysis and security risks evaluation. And by recognizing the risks areas, suitable controls will be chosen in order to reduce the identified risks effects.

So far, different methods and standards have been introduced to assess security, but none of them presents a systematic framework and method for assessing security and security risk optimum reduction.

In this article a framework is presented to evaluate shortcomings, holes and security risks along with an algorithm for optimum choice of risks reduction controls.

In the proposed framework standards and methods such as ISO/IEC 15408 Common Criteria for Information Technology Security Evaluation, ISO/IEC 17799, ISO/IEC 27002 security standards, Microsoft threatening model process and Use Case Function Point are used.

Key words: ISO/IEC 15408 standard, ISO/IEC 17799 standard, ISO/IEC 27002 standard, Microsoft threatening model, Use Case Function Point

1. Introduction

In recent years, we have been observing that more organizations are remarkably becoming dependent on informational systems [1].

Security discussions related to information technology are always a concern and a challenge to the security decision marker officials.

Security needs are usually considered as non functional needs for software development, and this will result in software security defect and the problem is growing [2, 3, 4].

In fact, a security defect is a kind of security rule breaking based on security policies which include the access or the lack of access to the sources in a report revealed by white hats security organization which was done to evaluate 2000 websites from Jun 2006 until Feb 2008, 9 out of 10 websites involved at least a security failure.

According to the CERT/CC report, the number of the software defeats related to the security have increased by five times in the past 7 years, whereas software failures results in the organization annual salary loss up to about 2% to 3% [4].

Security failures in software systems are problems that we hope to stop and this happens while safety scales for a system covers other system scales [5]. So, this matter over emphasizes the necessity for investigating the software systems security evaluation.

None of the methods and standards that have been presented up to now can express a systematic framework and method.

The proposed frame in this article, using the powerful points of present methods and standards, presents a systematic and useful frame which covers present methods shortcomings and relies on identifying and controlling risks optimally in order to evaluate the applications of security software.

In section 2 we focused on investigating different methods of security evaluation. In section 3 the proposed frame general information is presented. In sections 4 to 10 each stage of the frame and the conclusion will be present at section 11.

2. Different methods of security evaluation

In recent years, various evaluation methods and standards have been presented for investigating software security, each of them is prepared based on view, concept and special software characteristics. Some of them have more usages and are usable for a wider range of software systems.

2-1.ISO/IEC 17799 standard

ISO/IEC 17799 is an international standard which was taken from *BS 7999* in *2000* for the first time and its last edition was published in 2 parts in 2005 under the title of *ISO/IEC 17799:2005*. The goal of this standard publication is to give some suggestions in management information security filed in order to design, implement, security problems backup, evaluating the amount of the organization security and presenting useful methods to upgrade security in an organization. The mentioned standard is the starting point to develop organizations security methods [6].

1. One of the disadvantages of this standard is that only general topics and subjects are covered.
2. Also, this standard does not present any method for estimating operational costs of the risk control.
3. This standard does not recommend any metric to evaluate security.

2-2ISO/IEC 27002 Standard

In 2007, the last version of *ISO/IEC 27002* standard, as the most complete and comprehensive standard for the information security management system, was published by technical committees of *ISO* and *IEC* cooperatively.

This standard presents an effective model to accomplish goals such as control evaluation and estimation of the risk, design and implementation of the security and security management and review [7]. In both mentioned standards the *PDCA* (plan_ do_ check_ action) model is used to achieve the goals. In fact, the present management approach of both standards are based on management standard of *ISO/IEC 15939* [8]. And the following cases can be expressed as its short comings:

1. In this model, in last stages (*Act*) if it needs to adapt will be back to (*Do*) stage, however the primary goals may change. So this model has a problem with feedback.
2. The usage of PDCA cycle has extended because of its simplicity although in complex projects it is not useful [9].
3. Data store is full of obtained information from performing each stage of *PDCA* in *ISO/IEC 15939* model, all information and results taken from evaluation stage will be stored in data store without updating information, so the data store becomes very large and retrieving information from it will be costly.
4. Also, in this model we suppose that very thing starts by planning which causes limitation.
5. Since, *PDCA* cycle lacks measurements in the last stage it has been used less in recent years.

2-3.*ISO/IEC 15408 Standard*

The last version of standard with the same scales *ISO/IEC15408* was published in 3 sections in *2009*. This standard presents some metrics by which users can implement security needs in their products and evaluators can evaluate what producers claim about their products. This standard presents scales in 7 levels for evaluation. This standard involves some concepts such as:

Target of evaluation (*TOE*): is a software collection - a software or middleware with its related guidance documents that is a subject of an evaluation.

Protection Profile (*PP*): is a set of operational needs for a group of TOE products, which are independent from implement and satisfy customer's specific needs.

Security Target (*ST*): Are a set of security needs and characteristics that are used as a base for TOE evaluation [10]. For evaluating a product, a security company should present its product (*TOE*) security characteristics based on PP and ST [11].

We can point to the following cases as shortcoming of this standard:

1. This standard does not express the relationship between evaluation metrics and levels of software of the software lifecycle.
2. It cannot express the way to extract the security threats.
3. It cannot express they way to extract more metrics for higher levels evaluation.

2-4. Open Web Application Security Project

The Open Web Application Security Project is a large community that is supported by companies such as: *FOUMDSTONE*, *DELOTTE* and *VISA*, its goal is to provide suitable fields for organizations in order to enable them to develop trustable software or to buy and keep them. This project gives sufficient information and training related to the most vulnerable web applications. Architects, designer and software developers also presents a series of methods to protect them.

3. The proposed security evaluation frame general information

Security is a complicated characteristic and for assessing the security of the system we need to consider lots of opposing factors [12]. Many of the software functions without paying attention to the security services such as: integrity, availability, confidentiality have been developed. In the proposed frame of extracting security needs to complete *PP* and *ST* concepts such as generality; integrity, availability and confidentiality are considered as three main criteria of the security metric in functional systems.

The proposed frame has used the *ESA* standard to match evaluation approaches to the stages of the software lifecycle.

The first version of *ESA* engineering software standard was published in 1984 by the European space agency. This standard presents a concise definition about the production way of optimal software and by acceptable quality is produced. This standard involves three sections those includes product standard, method standard and attachment. Using the strong points of the present methods, the proposed frame presents a particle and operational way in order to assess the software functions, in a way that covers all the previous methods shortcomings.

The proposed frame expresses evaluation 7stages as follow:

1. Defining the security scales.
2. Creating management system of information security.
3. Determining sufficient documents to assess each stage of software lifecycle.
4. Recognizing evaluation stage and validity along with needed tests in each part of the product life cycle.
5. Doing risk evaluation.
6. Choosing and performing controls.
7. Adjustment of involving and audit document

4. Security indexes definition

The proposed frame in order to determine the necessary security is based on the suggested scales of the *ISO/IEC15408-2* standard also suggests the strong *E4* approach to extract any extra metrics [13]. *E4* is a cycle approach to extract metrics that its stages are shown in figure (Fig.1).

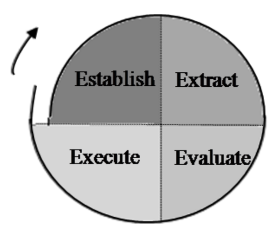

Fig 1: Four steps of E4– process[14, 15]

Related activities of each part of *E4* cycle are mentioned bellow:

1. Establish phase: The first step in any measurement activity is to establish a group of goals which should be accomplished.
2. Extract phase: Next stage of the measurement is extracting information.
3. Evaluation phase: After extracting information, assessing the information beings.
4. Execute phase: After finishing previous stage, it is time to make decisions and to perform them.

5. Creating management system of information security

Creating management system of information security must be done for performance, Management, backup and progress of the information security in organization. The presented framework using a standard method of *ESA* software engineering standard and benefiting *E4*, presents a pattern to create management system of information security which does not have shortcomings of the other standards. In figure (Fig.2) the proposed pattern is shown.

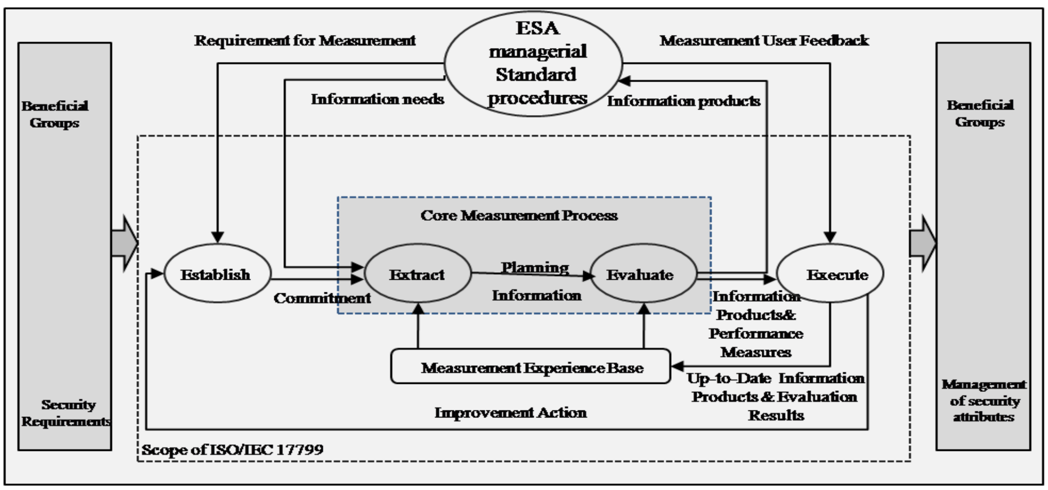

Fig 2: Management system of the information security pattern.

Characteristic of the proposed pattern for repairing managerial security system shortcoming of other standard is as follows:

1. In this frame, the feedback is considered to be from the performance stage to the beginning of the cycle (*establishment stage*).There for, even if in the middle of the task the goals change we will face no problems.
2. The proposed framework besides its simplicity can be used in large projects.
3. The proposed model in this pattern causes storage update keeping which results the storage capacity of the data store to decrease and therefore faster and more suitable information retrieval. Also, what is stored in storage can be used as on experience in next projects and also shows the organization perfection.
4. The proposed model core is based E4 instead of old cycle *PDCA*.

6. Needed documents in order to assess each phase of software lifecycle

The proposed frame presents needed documents for assessing security in each phase of the software lifecycle, by using product standard and *ESA* engineering software standard.
In figure (Fig.3) Phases of the product standard and needed documents in each phase are presented.

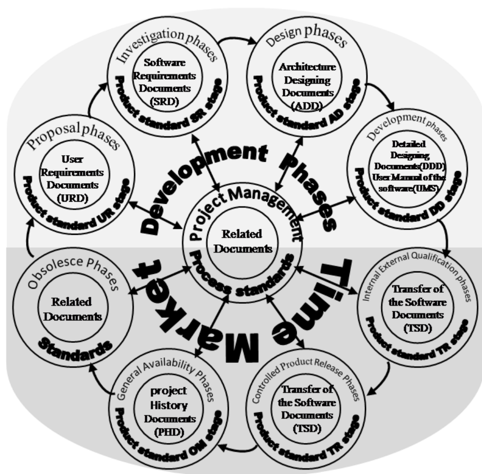

Fig 3: Matching phases of product life cycle to phase of ESA product standard[16].

7. Determining the stages of evaluation and needed tests in each phase of the product life cycle

The proposed frame expresses a written form of different phases of the Open Web Application Security Project with the phase of the product standard, in standard as evaluation stages. In figure (Fig.4) this matching is shown.

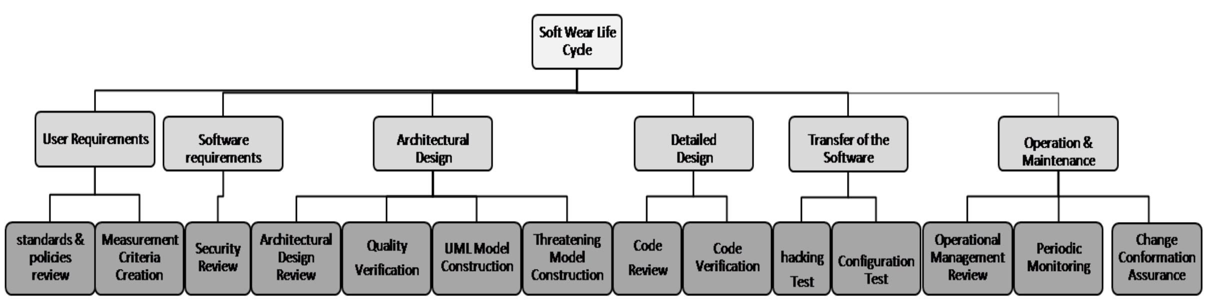

Fig 4: Matching phase of the Open Web Application Security Project to phase of product standard in ESA standard [17].

8. Security risks evaluation

The proposed frame is about risk management this is implemented through creating risk management system and based on the reduction strategies and via this, properties, threat and weak points can be determined and suitable quality level will be recognized and then controls will be chosen to neutralize or reduce the unpleasant risk to an acceptable level.

Risk evaluation stages are as follow:

1. Recognition of the properties in the security domain: security is related to the properties protection against threats, so to assess security we at first, should know properties and related threats. In proposed frame to prepare *TOE* in order to assess risks, properties should be known.
2. Determining the threats which are related to properties and vulnerable points of the properties: threats modeling method is an engineering tech.nic that helps a system designers to determine threats, attacks and vulnerabilities in software domain. Figure (Fig.5) shows procedures of the threats modeling based on the Microsoft threats modeling method.

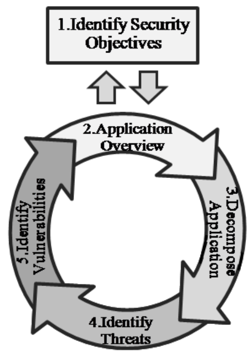

Fig 5: Circular method stages of the threat modeling.

Vulnerable points are shortcomings and lacks which are recognized in properties and using them threats cause risks. It is necessary to mention that a property may have different vulnerable points.

3. Determining real probability: real probabilities of each compound (*threat* + *vulnerability*) must be recognized. Compounds will unnoticeable probabilities will be ignored. Table (1) is used to determine incidences occurrence probability.

Grade	Frequency	Occurrence probability
0	Unlikely to occur	Unnoticeable
1	Two to three times in five days	Very low
2	Once a year ≤	Low
3	Once in six months ≤	Average
4	Once in month ≥	High
5	Two to three times in five days	Very high
6	Once a day	Unlimited

Table 1. Determining the probability of the event.

4. Unpleasant effect calculation: The unpleasant effect may be measured by numbers in order to show the caused damages by them.

This amount makes the risk important possible, ignoring its probability. The unpleasant effect is not dependent on probability table (2) is suggested for calculating incidence effect domain.

Grad	Unpleasant effect degree	Each incidence

		unpleasant effect
0	The least unpleasant effect or neutral	Unnoticeable
1	It needs lots of work to correct	Low
2	Unpleasant effect is remarkable	Remarkable
3	It is too costly and influences organization self confidence	Damaging
4	Cusses the loss of information for a long time and effects a large amount of the information and communication	Serious
5	Complete failure and unpleasant effect will take over all the organization	Dangerous

Table 2. Determining the events effect area.

5. The main goal of security evaluation is to calculate and decrease risk. With matching language risk can be expressed as what is presented in equations (Eq.1)

$$risk=probability * unpleasant\ effect \qquad (1)$$

Grad (probability * unpleasant effect)	Risk calculation
None	0
Low	1-3
Average	4-7
High	8-14
Crisis	15-19
Unlimited	20-30

Table 3. quantity calculation of the risk

The results of this calculation show the numerical evaluation of the properties risks for a specific set of threats and vulnerable points.
This numerical view is used as one of the factors for determining risk reduction of limited resource preferences.

9. Choosing and performing controls

The proposed framework suggests the risk reduction controls which are present in *ISO/IEC 17799* standard to reduce risk.
It's clear that organizations resources are limited to reduce risk, so we have to reduce some risks. Since all organizations tend to get more benefits the proposed framework presents a procedure for upgrade choosing of the risks reduction controls based on complete cost of each control and risks importance degree. To tell this, first risk reduction controls cost estimation method is expressed then an algorithm is presented for upgrade choosing.

9-1. Risk reduction controls estimations method

So far, several methods have been presented to estimate costs. One of these methods is cost estimation based of functional points which is very complicated [18]. The proposed framework suggests use case function point which is derived frame function point method to estimate the costs of the things done against risks. The output of this method is to estimate the procedure based on person in day that with the consideration to each person payment the total cost of a (*UCFP*) can be calculated.

9-2. Upgrade choice algorithm to reduce risk

The main goal is to spend the budget of risk correction in organization in a way that result in the most advantage. Generally the overall problem domain is as follows:
An organization with budget (B) and N recognized risk domains for, which the cost of any done action to confront each risk (R_i) is estimated (C_i) by (UCFP) method, and its value is consider as the resulted amount of the calculation of the risk domain (P_i).So, it's clear that the sum of the actions cost for the chosen risks should not exceed this risk correction budget. In more exact words the goal of making maximum the quantity:

$$\sum_{i=1}^{n} PiRi \tag{1}$$

If:

$$\sum_{i=1}^{n} CiRi < B \tag{2}$$

$$0 \leq Ri \leq 1 \qquad 1 \leq i \leq n \tag{3}$$

In optimum choice, first an increasing N number array, based on value ratio on (Pi/Ci) cost, is produced and then we make our choice based on the following algorithm:

```
Procedure Greedyselect(Pi:myarray;Ci:myarray;Ri:myarray;n:integer;B,Profit:real)
var CU:integer;
begin
  Ri=0;
  Profit=0;
  CU=B;
  for i:=1 to n do
    begin
      if Ci[i]>CU then
      Ri[i]:=1
      CU:=CU-Ci[i];
      Profit:=Profit+Pi[i];
    end;
  Ri[i]:=CU/Ci[i];
  Profit:=Profit+Pi[i]*Ri[i];
End;
```

This algorithm order is equal to (*n log n*) if sorting time is counted.

10. Adjustment of involving and audit document

After preparing *TOE*, *PP* and *ST* evaluation stage should be done. Security evaluation is an activity that is done by evaluator in order to assess *ST* security goals of the possessions *(TOE)* and finally in a document which is called protected profile *(PP)* the security degree of *TOE* is mentioned.

11. Conclusion

In this article, we investigated the present security evaluation methods and standards in which the weak and powerful points of them was mentioned. Then, a framework is presented for assessing functional software security. The proposed framework in this article has comprehensive and systematic characteristics and is methodological and usable. Analyzing

the present evaluation method, makes use of their positive properties and needed presents sufficient strategies to full fill their shortcomings. This article, with the aim of maximum usability, specifically uses the evaluation standard of the same scales as the base for conceptual classification and then presents all activities and documents which are needed for security evaluation of each stage of the software lifecycle. The proposed framework presents a special pattern, with consideration to managerial procedures importance for improving the evaluation function that does not have the shortcomings of the present management security methods. Some of the extra ordinary characteristics of the proposed framework to which we can point out are its focus on the risk reduction optimally and its being systematical.
To do some activities of security evaluation of the software functions we need some presuppositions, the suggested framework includes these presuppositions.
The suggested framework has a special kind of generality, as it introduces all present security mechanism of the functional programs which should be investigated by an evaluator, in a hierarchical way.
With consideration to the extra ordinary characteristics of the suggested solutions, it would be possible to establish operational sets to evaluate the security of the software functions.

References

[1] Mellado.D., Fernández-Medina. E., M.Piattini.(2007). A common criteria based security requirements engineering process for the development of secure information systems. ComputerStandards &Interfaces29, pp. 244-253.

[2] Talukder. A. K., Chaitanya.M. (2008).Architecting Secure Software System.

[3] Shina.M.E., Gomaa.H.(2007) . Software requirements and architecture modeling for evolving non-secure applications into secure applications., ScienceofComputerProgramming66, pp.60-70.

[4] Chowdhury.I., Zulkernine. M.Using.(2010). complexity, coupling, and cohesion metrics as early indicators of vulnerabilities .,JournalofSystemsArchitecture, pp.xxxxxx.

[5] Veiga.Da., Eloff. J.H.P.(2010).A framework and assessment instrument for information security culture “computers & security 29, pp. 196_207.

[6] ISO/IEC 17799:2005, International standard Organization, Information technology- Cod of practice for information security management.

[7] ISO/IEC 27002:2007, International standard Organization, Information technology- Cod of practice for information security management.

[8]ISO/IEC15939:2007(E),International standard,Systemsand software engineering-Measurement process.

[9]Bégnoche.L., Abran.A., Buglione. L.(2007) .A Measurement Approach Integrating ISO 15939, CMMI and the ISBSG.

[10] ISO/IEC 15408-1:2009-12-15,Information technology _security techniques_Evaluation criteria for IT security Part1:Introduction and general model.

[11]ISO/IEC 15408-3:2008-08-15,Information technology _security techniques_Evaluation criteria for IT security_Part3:Security assurance components.

[12] Sommestad .T., Ekstedt .M., Johnson .P.(2010). A probabilistic relational model for security risk analysis “computers & security 29, pp. 659–679.

[13] ISO/IEC 15408-3:2008-08-15,Information technology _security techniques_Evaluation criteria for IT security _Part2:Security fanctional components.

[14] Davami .F., Ali Mohammad Malayeri .E., Modiri .N.(2010).A Framework for Software Measurement Based on Managerial Procedures and Standards., 1st National Conference on Soft Computing and

Information Technology, Iran. Mahshahr .

[15] Davami .F., Ali Mohammad Malayeri .E., Modiri .N.(2010).A Framework for Software Measurement Based on Managerial Procedures and ISO/IEC15939 Standard, Function Point .3st National Conference on Soft Computing and Information Technology, Iran .Hamedan .

[16] Modiri .N., Davami .F., Ali Mohammad Malayeri .E.(2010).Software Metric .pp.31-38.Iran-Tehran.

[17] Ali Mohammad Malayeri .E., jabbehdari.s, Modiri .N., Davami .F. (2011). A Framework for the Evaluation of Security Defects and Vulnerabilities of Software Applications. Conference Software Engineering , Iran. Gonbadkavus.

[18] ISO/IEC 19761:2003(E), International standard, Software engineering - COSMIC-FFP – A functional size measurement method.