Risk Management in the Process of Risk Analysis

František Zbořil
Petr Hanáček

zborilf@dcse.fee.vutbr.cz
hanacek@dcse.fee.vutbr.cz

Abstract: Risk analysis is one of many tools for security improvement. The main idea of it is based on analysis of gathered information about an observed company and following searching for some group of countermeasures which can reduce a risk. The paper discuss inference mechanisms in the process of Risk Analysis called Risk Management. The progress is demonstrated by one example.

Keywords: Risk Analysis, Risk Management

1. Introduction

Several last years brought outstanding ascent of computer usage all over the world. The computers have become to be very significant part of life. This phenomena causes need for higher level of security. One of the tools for improving the security is a problem of risk analysis. Risk analysis studies an observed object (for example an company) and tries to find out some risks which endangers the object. These risks are mostly analysed on the basis of the company examining as a set of entities with some weaknesses which could be exploited to cause some loses. This text discuss one way how to proceed the process of risk analysis and shows an application by an example written in the Prolog language. Prolog as a member of the logical language family appears to be good programming language for artificial intelligence. It may be found that Prolog is a suitable instrument for an implementation of the knowledge based systems, too.

2. Risk Analysis

The process of Risk analysis can be divided into two parts. The first part of this process establishes a model of an observed system. This is mostly done by filling out a set of questionnaires about a subject of interest (company, institution etc.). This information can be divided into three groups – information about *assets* (computers, buildings, data; the attribute is price of the asset), information about *threats* (probability of threat realisation) and *vulnerability* (some level of asset's weakness for each asset). Risk is then obtained from this data. In fact, risk is considered as a probability that a threat will be realised through a vulnerability of an asset. The level of the risk is then estimated on basis of previously mentioned attributes. As an example, let us consider that a building is endangered by fire and from questionnaires was found that the fire protection is provided poorly. Thus there are serious risk that the fire disaster can cause some losses. Another example can be a contingent misuse of data stored in a computer by an unauthorised person. To decide whether there is really such a risk it is appropriate to inspect how is the data protected, who has access to the server room and so on. When all the risks are found the second part of this process begins with searching for a group of countermeasures which could reduce the unfavourable effects of the risks. Figure 1 shows the whole process of risk analysis.

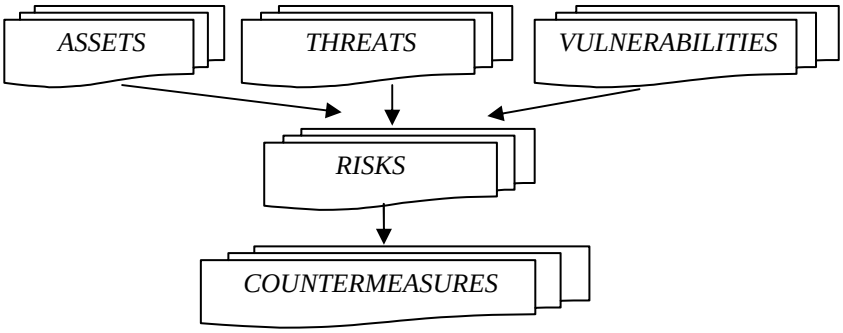

Figure 1 Process of Risk analysis

More detailed algorithm of complete process of risk analysis follows:

1. Identify all the assets included in the observed system.
2. Evaluate these assets.
3. Identify asset's vulnerabilities.
4. Retrieve threat and estimate likelihood of associated vulnerability.
5. Find all possible risks to the assets.
6. Propose countermeasures that can prune the risks.
7. Examine proposed countermeasures and make a decision of its applicability to the system.
8. Implement chosen countermeasures.

This text focus attention on the second part of risk analysis (5, 6 and 7 above paragraphs) - selection of proper countermeasures. But it is suitable to show how to build the model of an analysed object first. Next section describes the structure of this model.

3. Model establishing

As was mentioned above there are three major entities (four together with risks) involved in the process of risk analysis. It is obvious that information about assets threat and vulnerabilities must be stored in some form in a computer. Let us consider that there is a system which establish such a model and the results are kept in the form of database tables. Most of operational systems allows comfortable work with data stored in database tables. So probably there will be three tables, one for each entity. Each entity should contain its primary key and name. In addition all of the entities have their own attribute.

An attribute of an asset is its price. The representation of prices can be done by expressing their values in some currency (pounds, dollars). Another method is to input the price as a number of some range, for example from 1 to 10. Then each value from the range represents some scale of the price (1 means $1 to $100, 2 means $100 to $ 500 and so on).

Thread's attribute is likelihood of its occurrence. Expressing of this quantity is little more difficult than it was in the case of assets. There is usually a set of questionnaires used in the process of evaluation of thread's likelihood. Questions are formed so that it is possible estimate the number of occurrence of a threat per year (*Could replay of data in transit result in direct financial or non-financial benefit / reward for contracted service provider? Could delivery out of sequence result in direct financial or non-financial benefit / reward for contracted service provider?*). There are some predefined answers which contain a values which correspond to the scale of thread's likelihood. It means that the likelihood of previously mentioned threat is higher when a person responsible for fulfilling the questionnaires answers that there can be an profit for somebody when sequence is not delivered in proper order. Total likelihood is then counted as an average value of all the questionnaires focused on given risk.

Finally there are some vulnerabilities which can be exploited to cause a unpleasant effect. A vulnerability is bounded with an asset and means an assets weakness which can be exploited by an threat. The level of each vulnerability is again estimated using questionnaires. The questions are formed in such a way that they can discover and evaluate the scope of the vulnerability (*Have any people working for contracted service provider been warned, disciplined or prosecuted in related to internal confidentiality rules, the Computer Misuse Act or other legislation?*)

Following figure shows the data structure and interconnection among entities after the process of analyse.

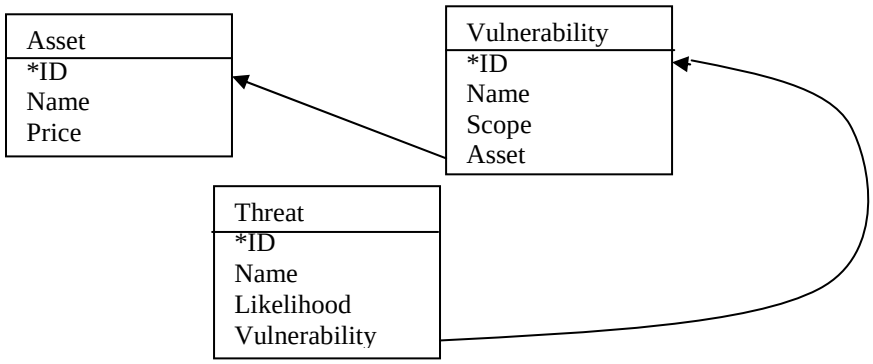

Figure 2 Data structure and interconnection among entities

Tables are the result of process of model establishing and they are assigned to the second part of risk analysis. This part is called risk management and its aim is to find out and propose some countermeasures which can reduce discovered risks.

4. Risk Management

Before some countermeasures can be proposed it is necessary to identify all significant risks in the system. Also there must by some knowledge about all possible countermeasures. System performing risk management must know which risks can the given countermeasure reduces, how much it reduces each risk, expenses for maintaining of the proposed countermeasure and so on. Then the system must be able to propose some decision. Generally the process of risk management can be divided into following stages:

1. *Risk identification.*
2. *Searching knowledge base for countermeasures.*
3. *Selection an appropriate combination of countermeasures.*

The first and relatively the easiest step, which the inference mechanism has to do, is risk identification. All risks in the system must be discovered and evaluated. A risk will be found if there is an asset which has a vulnerability, and there is a risk to the vulnerability. The process will subsequently browse through all assets. For each asset it will look for every threat that can be realised through some of the asset's vulnerabilities. Apparently all the risks can be identified. The problem is how to establish a level of risks. Level of a risk that some threat with high likelihood will be realised through vulnerability with high scope is also high. This value will be important later during the stage of selection of countermeasure when only the countermeasures with higher or equal level can be accepted. Price of an asset which is endangered by such a risk is important for decision whether the countermeasure does pay off or not. Usually there exist some table which assigns risk level for each pair of threat likelihood and vulnerability scope. But in some cases it is enough to compute this value as:

Risk Level = TRUNC((*Threat Likelihood* + *Vulnerability Scope*)/2)

Obviously there will be found risks with level from 1 to 10????. In this stage some risk whose level is under a considered level can be omitted. Now there is a list of risks. Each item – risk contains information about which asset is endangered with the risk, through which vulnerability a threat can be realised and what is the level of the risk. Such a list is shown in the following figure.

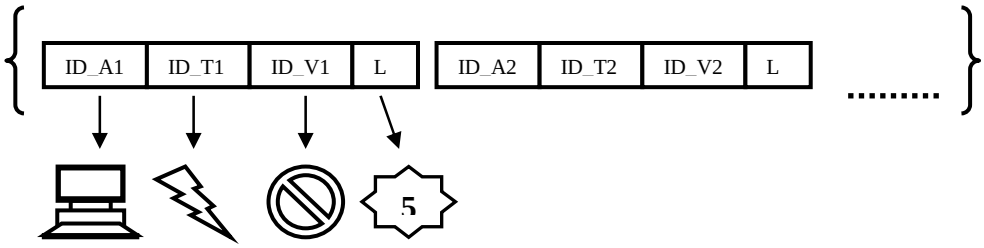

Figure 3 Structure of the list of risks

Now it is suitable to introduce representation of countermeasures. There are three significant attributes which countermeasures must contain. At first every countermeasure must hold information into which risks the given countermeasures can be applied. The second attribute is a contribution of the countermeasure. As was mentioned before every risk has a level and only the countermeasures with equal or higher level can be applied. Last attribute is a price of the countermeasure. The value of the price must correspond to the value of asset's price. Probably it is nonsense to propose such a countermeasure whose expenses for maintaining are higher than price of an asset which this countermeasure should protect.

When there is a knowledge about all the risks which are possible to implement the system is ready to search this knowledge and find out all possible countermeasures for all discovered risks. In this stage it is not important whether a countermeasure pays off or not. The only condition is that the level of countermeasure must by higher or equal than level of risk. Requested result of this step is to assign, for every risk found in the observed system, all possible countermeasures which could prune or reduce it. Obviously in many cases, there are more than just one possible countermeasure for a risk and a countermeasure is able to reduce more than one risk.

For example there have been found four risk, let us denote them R1 .. R4. Each of them endanger an asset whose price is 50. Also there have been found five possible countermeasures. These countermeasures and the associated risks are denoted as:

Countermeasure([Risks(Price of asset)],Total price of assets, Expenses)
[C1([R1(50)],50,40)
C2([R2(50)],50,40)
C3([R1(50),R2(50),R3(50),R4(50)],200,150)
C4([R3(50)],50,40)
C5([R4(50)],50,40)]

The last stage of the process of risk management is to find such a combination of countermeasures that covers, if it is possible, all the risks with the lowest expenses. This is a typical task that can be solved by using by artificial intelligence tools. It is possible to use some algorithm of state space search like uniform cost search, iterative descent depth first

search or backtracking. But the problem is that it is rather difficult to find the optimal solution. Thus it can be said that the solution is acceptable when total expenses do not exceed some predefined amount. Then the algorithm may be in the following form:

There are two lists used throughout the algorithm. The first one is the input list established during the process of the searching knowledge base for countermeasures. The second list is called "Solution list" and at the beginning it is empty. When the algorithm finishes, the solution list will contain the proposed countermeasures.

1. *Clear the solution list.*
2. *If the input list is empty, no solution can be reached, stop the algorithm.*
3. *Select the next item from the input list and add it into the solution list.*
4. *Reduce remaining items in the input list by the risks involved in the selected item.*
5. *If the total expenses exceeds a predefined expensess remove the last item from the solution list, re-compute back the input list and go to step 3.*
6. *If the input list is not empty, go to step 3.*
7. *If the solution reduces all the requested risks propose a solution.*

Step 4 means that when a countermeasure is added into the solution list (it is thought to be proposed) the input list must be recounted. There will remain only the countermeasures which could cover an uncovered risk. In contrary when a countermeasre is removed form the solution list (step 5) the input list must be recounted back.

The graphical form of this algorithm is shown in the following figure. Maximal expenses of 50 are thought there. It is consequently selected the first three countermeasures which reduces all the risks R1 to R4. But the total expenses are 70 what is more than was expected. Thus there is need to try to find out another solution with a lower expenses. Such a solution is to propose countermeasures C1,C2,C4 and C5. But although it is acceptable solution, it is not optimal. The optimal solution is to propose countermeasure C3 which covers all the risks and the expenses are only 30.

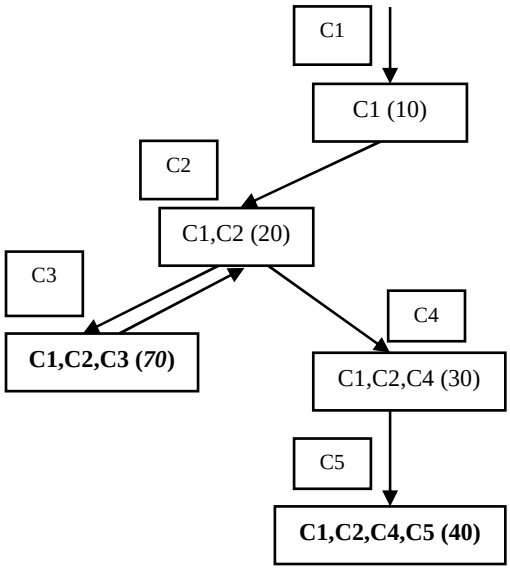

Figure 4 Diagram of process of countermeasure proposal

An example of an implementation of the algorithma is mentioned in [3].

5. Conclusion

Unfortunately, the problem of Risk analysis is more complex than could be described in this text. There was demonstrated only one possible approach to the problem …

Bibliography

[1] Pfleeger ,Ch.P.: Security in computing, Prentice-Hall, Inc. ISBN 0-13-799016-2

[2] CRAMM Management Guide

[3] Zboril ,F.: Risk analysis and management methods, Master Thesis, FEI VUT v Brně, 2000