Imed EL FRAY
ZACHODNIOPOMORSKI UNIWERSYTET TECHNOLOGICZNY, WYDZIAŁ INFORMATYKI,
ul. Żołnierska 49, 71-210 Szczecin

An approach to determine the Evaluation Assurance Level to the system based on the results of risk analysis

Ph.D. eng. Imed EL FRAY

Imed El Fray, PhD, Eng. is employed at the Chair of Software Programming, Department of Computer Science, The West Pomeranian University of Technology in Szczecin. The main research area is the risk analysis, information security and management, system and application security evaluation.

e-mail: ielfray@wi.zut.edu.pl

Abstract

This paper presents an approach to determine the Evaluation Assurance Level (EAL) for IT systems based on risk analysis results with the use of common methods, such as CRAMM, OCTAVE or MEHARI. The main goal of the work was the analysis of mutual influence of strength of function and vulnerability taking into account the classification of common vulnerabilities. The attack potential factors were also determined as elements broadening the knowledge bases included in Mehari method. The correctness of discussed method has been verified on the example of CA computer network.

Keywords: risk analysis, evaluation assurance level, strength of function level (SOF-Level).

Sposób wyznaczania poziomu uzasadnionego zaufania do systemu w oparciu o wyniki analizy ryzyka

Streszczenie

W artykule przedstawiano sposób wyznaczania poziomu uzasadnionego zaufania do systemu (EAL) w oparciu o wyniki analizy ryzyka z wykorzystaniem dostępnych na rynku metod analizy ryzyka, jak CRAMM, OCTAVE czy MEHARI. Głównym celem pracy była analiza wzajemnego wpływu siły funkcji zabezpieczeń, potencjał ataku, oraz komponenty procesu analizy podatności z uwzględnieniem klasyfikacji powszechnie występujących słabości systemów informatycznych. Określono również czynniki potencjału ataku jako elementy rozszerzające bazę wiedzy zawartą w metodzie Mehari. Prawidłowość omawianego sposobu zweryfikowano na podstawie przykładowego sieciowego urzędu certyfikującego (dwusegmentowa sieć CA). Otrzymane wyniki wykazały, że przy minimalnych zmianach w bazie wiedzy Mehari możliwe jest wykonanie szczegółowej oceny badanej przykładowej infrastruktury klucza publicznego oraz w przybliżeniu można wyznaczyć jej poziom uzasadnionego zaufania zgodnie z wymaganiami wspólnych kryteriów (Common Criteria ISO/IEC 15408).

Słowa kluczowe: analiza ryzyka, poziom uzasadnionego zaufania, poziom siły funkcji zabezpieczeń.

1. Introduction

Organizations using common standards are usually observed as more reliable. An achievement of the agreement with standards allows more effective organization of the work and access to the knowledge and experience of the experts. The examples of the utilization of such standards as quality, security and trust to IT system measures, can be the requirements of certification organization according ISO/IEC 27001, 15408 [1,2] standard.

An achievement of agreement with the standard is a long lasting process where many efforts of organization personnel are required. The main problem with the evidence of conformity is the necessity of complying oneself to regulations, criteria and creation of essential documentation, proofs, etc.

Taking into account the similarities and differences in requirements, criteria etc. associated with the certification according ISO/IEC 27001 and 15408 standards, an effort was made to create an approach enabling to achieve the defined approximate level of EAL to IT system based on risk analysis results. Due to combining the advantages of both above mentioned standards, this approach allows in details to identify the potential threats and susceptibility of assets, to determine the risk seriousness for different scenario, to analyze the implemented security mechanisms or select the new one, depending on the risk seriousness, and to determine the EAL level for all these mechanisms.

2. Risk analysis

According to ISO/IEC no 73, the risk evaluation is defined as a process composed of risk analysis and evaluation [3]. The risk analysis process is aimed at determination of uncertainty level of endangered organization [2, 3, 4]. The degree of uncertainty can be connected with the area of organization activity or its information systems security.

Considering the results and probability of risk occurrence, one can define priorities for detailed analysis. According to [4], the risk evaluation is an important basis for making decision whether given risk is significant for organization and necessary to be taken into account and what type of activities are needed to be made.

Considering the above processes of evaluation and methodology according [1], it can be concluded that this process is focused not only on specific security measures but also on the entire system environment. This imply situation where realization of undeniable requirement of security information, e.g. information through the wide array of security mechanisms supported by standard risk analysis cannot be sufficient for the evaluation of their resistance to attacks and determination of the strength of security functions.

3. Trust building

The lack of evaluation of the system resistance to attack is creating an uncertain situation. Such uncertainty of the system is caused by the lack of trust to the system, and indirectly arises from its security measures. In order to create the trust to the system, evaluation of this system has to be made. Such evaluation can be made with the use of common criteria (CC) [5, 6, 7]. The CC standard makes available different mechanisms, functions, requirements, etc, which need to be taken into consideration during the system design. They can also serve as a tool for monitoring different threats and complying resistance of evaluated mechanisms or functions to attacks with the use of specific threat.

Due to the above mentioned possibilities within CC and possibility of additional standard risk analysis as described in section 2 for remaining phases, an attempt to define an approach has been made and presented below.

4. Proposed approach

Proposed approach is based mainly on the attack potential, which constitutes an element combining vulnerability of proposed security mechanisms (as result of risk evaluation) with the strength of security functions, and indirectly with level of EAL.

General scheme of proposed approach is presented in Figure 1.

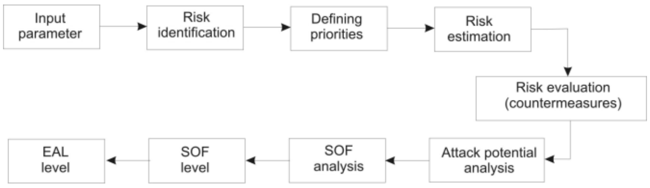

Fig. 1. General scheme of proposed approach
Rys. 1. Ogólny schemat proponowanego podejścia

The approach determining the EAL to the IT system, depending on the results of risk analysis should be continuous, recurrent and iterative process taking into account all phases of the life cycle of the system. According to Fig. 1, in initial phase, the resource assets, threats and vulnerabilities should be identified and classified. For vulnerabilities recognized as critical, appropriate risk scenario should be defined for those which may pose the risk to assets and can have indirectly a negative influence on system security.

Referring to the process of vulnerabilities analysis, and specifically to its result, one should acquire the list of potential weaknesses with indicated, so called, critical vulnerabilities. Determination of critical vulnerabilities has a great significance for ascribing priorities to individual identified risks. For this purpose, available tools or methodologies such as Cramm [8] or Mehari [9] can be used.

Risk minimization with the use of this tool is usually a final stage of standard risk analysis. However, in proposed approach, the risk analysis process is continued because countermeasures are evaluated against the resistance arising from analysis to mass attack of different potentials in order to gain the trust for proposed and implemented functions, security mechanisms etc. The CC makes accessible different solutions and techniques to the estimation of attack potential. Tables 1 and 2 show the way to calculate the attack potential and the ratio of identified vulnerabilities to attack potential [7]. Table 2 illustrates the links between steps of proposed approach.

Process of analysis and estimation of attack potential should be carried out according to Tables 1 and 2 for every selected path of attack where identified vulnerabilities were not eliminated from previous stage of risk analysis as useful. If the attack is similar then it should be taken into account during evaluation and then analyzed. If the number of vulnerabilities or their mutual correlation makes impossible to perform the analysis of attack potential unambiguously, then the application of the tree threats [10] is recommended. The advantage of such solution is not only its transparency but also simple interpretation based on the case study, i.e. an assumption and investigation of efficiency of path attack. If new vulnerabilities are detected during iterative process of correlated weaknesses search in all stages of the method, the renewed analysis should be performed for new identified attack paths.

The last stage of proposed approach is the determination of the level of the strength of security functions against attack potential calculated from Table 1 and Table 2.

Indicated SOF level should reflect the worst of all the possible cases which were considered during the identification and evaluation of vulnerabilities and analysis of risk potential. Such assumption arises from the fact that if there are two different attack paths existing within two different levels of attack potential, then the case of the lowest strength of security function cannot be omitted because such situation could pose a falseness on real level of security mechanisms and similarly to the lack of iterative method could provoke the creation of illusory sense of security assets, for which safety is based on the strength of security functions.

Finally, determination of the Evaluation Assurance Level (EAL) to IT system, and precisely to its function or security mechanism stipulated during risk evaluation process is based mainly on the type of identified vulnerabilities and technique of risk analysis performance. Taking into consideration above relationship between the attack potential and the strength of security function which depends also from the type of identified vulnerability and technique of analysis performance, one can conclude that the EAL to the system depends also from the strength of security functions.

Tab. 1. Calculation of the attack potential value
Tab. 1. Obliczenia wartości potencjału ataku

Factor	Range	Value
Elapsed time Total time necessary to identify the fact that specific vulnerability can exist is the subject of evaluation, the method of evaluation and its successful realization	=< 1 day	0
	=< 1 week	1
	=< 1 month	4
	=< 3 months	13
	=< 6 months	26
	> 6 months	*
Expertise Knowledge referring to the level of general know-how of product type or attack method	layman	0
	proficient	2
	expert	5
Knowledge of product	Public	0
	restricted	1
	sensitive	4
	critical	10
Equipment Refers to equipment and software which is necessary for identification or utilization of vulnerability	standard	0
	Specialised	3
	Bespoke	7
Access to product	unlimited	0
	Easy	1
	Moderate	4
	Difficult	12
	None	**

* Indicates that the corresponding attack potential is beyond high attack potential
** Indicates that the attack path is not exploitable due to other measures in the intended operational environment of the TOE

Tab. 2. Detailed relationships between the individual EALs, components, attack potential and the strength of security function
Tab.2. Szczegółowa współzależność pomiędzy poziomem uzasadnionego zaufania EALs, potencjałem ataku, komponentami procesu analizy podatności a siłą funkcji zabezpieczeń

Process components of vulnerability analysis	Value range	Resistance to attacker with attack potential	minimum SOF level	Evaluation Assurance Level
AVA_VAN.1 Vulnerability review	0-2	no rating	no rating	EAL1
AVA_VAN.2 Vulnerability analysis	3-5	basic	low	EAL2
				EAL3
AVA_VAN.3 focused vulnerability analysis	6-9	enhanced basic	low	EAL4
AVA_VAN.4 Methodological vulnerability analysis	10-14	moderate	moderate	EAL5
AVA_VAN.5 Advanced Methodological vulnerability analysis	15-26	high	high	EAL6
	>26	beyond high		EAL7

4.1. Example of proposed approach

Fig. 2 shows an example of a secure CA network responsible for management and certificates service. As it can be seen from Fig. 2, that presented network is composed of two internal segments and fulfills the requirements of European Directive from 13 December 1999 [11] and requirements related to Firewalls between www servers and Internet. Server of Registration Authority (RA) and server of Trusted Third Party (TTP) are protected by standard firewalls characterized by EAL4 security level according to CC [12]. For evaluation of assurance level to IT system based on the risk analysis, the extended MEHARI method with basic criteria, requirements etc. according to CC requirements will be used.

4.1.1. Risk analysis and evaluation for exemplary CA computer network

From the technical point of view, analysis of the CA (implementation of the network structures which accomplishes individual functions of the PKI as demonstrated in section 3) as well as considering additional elements which are components of this infrastructure (policy, procedures,...), the disturbances and abnormalities in the functioning of individual components can be result of various factors, such as:

- disclosure of private key - possible in case of: personnel staff disloyalty, poor quality key, gaps in cryptographic devices storing private keys, incorrect configuration of devices, improper level of computers storing the subscribers private keys, etc.
- disturbances in the work of servers which are components of the PKI infrastructure - possible in case of incorrect configuration of servers, placing physically too many services on one server, improper monitoring of the state of security of individual servers,
- falsification of transmitted data - possible in case of improper security level, when communication channels between subscriber and server or registration point is not exploiting the encrypting process or are using weak encryption algorithms,
- disturbances of work of the network – possible in case of excessive loading, or the carrying out the attacks of refusal services (the attacks of DDoS),
- physical damage of hardware - possible in case of personnel staff disloyalty, as result of unaware mistake disabling continuation of the work etc.,

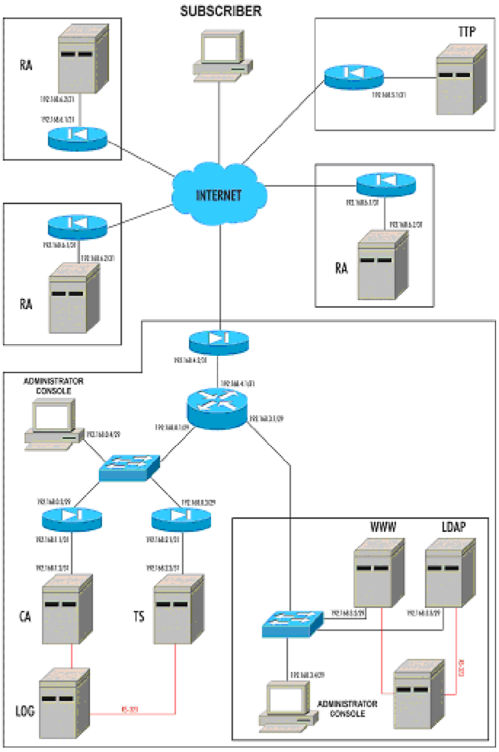

Fig. 2. An exemplary computer network of the CA utilized for the risk analysis
Rys. 2. Przykładowy sieciowy urząd certyfikacji CA użyty do analizy ryzyka

The calculation methodology for the estimation of impact and potentialty, and the method of identification and classification of resources is given in [9]. For the purpose of this paper and with the use of mathematical approach according the literature, the results of evaluation of the risk seriousness are represented in Tab. 3.

4.1.2. Assessment of assurance level to the PKI infrastructure

According to the description in section 4.1, the next step to determine the countermeasures is based on risk seriousness values from Table 3.

Tab. 3. Assessment of risk weight to the PKI infrastructure
Tab. 3. Oszacowanie wagi ryzyka dla Infrastruktury PKI

N^0	Scenario	Origin	Risk Level
S1	Destruction of hardware and software by:	water damage	2
		short circuit of power supply	2
		malicious (logic bomb), authorized person	3
		malicious (logic bomb) of non-authorized person	2
S2	unavailability to access the CRL or verification services regarding certificate status:	natural catastrophe	2
		conscious attack of third person or by authorized person	3
		software crash	3
		overloading of server	2
		breakdown of hardware discs	3
		breakdown of directory file service LDAP crash (CRL, keys, certificates)	2
S3	disclosure of private key by:	through intruder	2
		through software programmer (back door)	2
		through inlegally authorized personnel	3
		through telecommunication personnel (utilization of minitoring devices)	2
S4	Data manipulation (incorrect information about the time stamping)	outside intruder	2
		through personnel member manipulating network devices	3
		destruction of the atomic time pattern	2
		asynchronization of the atomic time pattern	1
S5	False verification of identity	malignant modification by programmists (eg. Software modification of CA server, repository server, LDAP which can result in issuing of incorrect certificates)	3
		false declaration (false identity card)	1

According to this table, seriousness for the majority of scenarios is at a tolerable level. However, for such systems as PKI, trust to the function and security mechanisms can be gained if the value is at a Low level. For that purpose, in order to justify proposed approach, only one scenario in this paper was analyzed (at the end of the sub-section presented in table 4 the result for all scenarios are presented):

- data manipulation by intruder acting from outside.

For the above scenario, data manipulation by intruder is technically possible (risk seriousness =2), if the adversary will achieve the user's password. Gaining the user password can be the result of i.e. application of weak mechanisms of verification and password generation or usage of socio-techniques by the intruder.

In order to achieve evaluation assurance level to verification mechanism and password generation used in exemplary CA network according to proposed approach, the attack potential for identified vulnerability should be calculated at first from Table1.

As it was discussed in section 4.1, the analysis process and estimation of attack potential should be performed for each attack path, where identified vulnerabilities were not eliminated. For the purpose of this paper, only one identified vulnerability was considered, namely "possibility to gain user's password", which is shown on above tree of threats (Fig. 3).

It should be pointed out that attack paths, where gaining user password is based on socio-technique, are eliminated because of the lack of appropriate security functions protecting the system against such activities.

Above examples of threats tree are not exhausting all possible attack paths because all presented potential vectors seem to be impossible at a large number of accessible tools and methods to break security. However, from our point of view, they are satisfactory for overall presentation of approach.

For the vulnerability "gaining user's password" and it's corresponding threats (an unauthorized user may gain unauthorized access to the system and act as the administrator or other trusted personnel due to failure of the system to restrict access, an unauthorized user may gain access to system data due to failure of the system to restrict access, a user may gain inappropriate access to the system by replaying authentication information, etc.), an analysis of attack potential was performed.

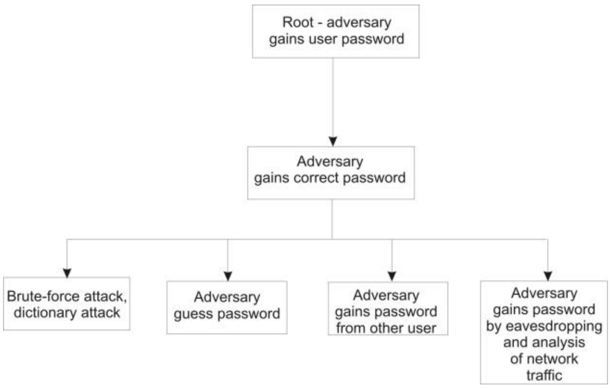
Root - adversary gains user password
Adversary gains correct password
Brute-force attack, dictionary attack
Adversary guess password
Adversary gains password from other user
Adversary gains password by eavesdropping and analysis of network traffic

Fig. 3. Tree of threats for „gaining user's password" mechanism verification of password generation
Rys. 3. Drzewo zagrożeń dla mechanizmu „przywłaszczenia hasła użytkownika" weryfikującego generowanie hasła

Special scenario assuming security domains described in section 4.1 and collecting appropriate data according to requirements as given in Table 1 was utilized for the evaluation process. The results of performed analysis (tests documentation, etc.) with shortened description are given below:

1. Run time: =< 1 month what refer to value: 4
Scanning with automatic tools for Users listing is less time-consuming. Selection of such time arises from the fact that performance of effective dictionary attack on the password is time consuming. This parameter, from potential adversary point of view, was considered as characteristic to the worst case. In case based on the assumption that the simple connotation or short passwords are used, the value of a parameter should be set as =< 1 week.

2. Expertise: proficient, value: 2
The level of this factor refers to an orientation in the functioning of protocols, applications and security of the system or mechanism evaluation and their configuration.

3. Knowledge of mechanism: public, value: 0
Taking into account such elements as universality of usage of the mechanism or professional training literature, an assumed value seems to be appropriate. Information resources referring to the construction and functioning of the system do not show detailed and complicated functioning mechanisms of system elements, which are responsible for providing security on implementation level.

4. Equipment: standard, value: 0
At the current assessable computational ability of processing units and their accessibility, the value of this factor was assumed as maximal and adequate for analyzed attack path. It should be noted, however, that equipment value can unambiguously be connected with the value of protected assets for the given mechanism. Therefore, taking into account current high level of information technology it should be assumed that the motivation of intruder will be high.

5. Circumstances (access to the mechanism): moderate, value 4
Considering actually used prevention measures, such as firewalls, antivirus programs, intruders and intrusion detection systems, assumed value for this factor seems to be appropriate. It is possible to connect multi-sessions or to obtain physical access to the equipment, however those are extreme cases.

Finally, according to Table 2, the summary value of individual factors: 4+2+0+0+4=10. From this value we can read from Table 2 the value of attack potential. According to this table, the investigated system is resistant to attacker with a **moderate** attack potential. In comparing the value of attack potential with the level of the strength of security function it was read from Table 3 that investigated system was characterized by a **moderate** level of the strength of security function.

Summarizing, performed evaluation for all identified vulnerabilities connected with exemplary CA network with the use of Mehari method showed **enhanced basic** level of attack potential (Tab. 4). It should be noted, that an analysis of the identified vulnerabilities was performed according AVA_VAN.3 requirements [7]. As can be seen from Table 4, the minimal level of the strength of security function is **low**, what refers to EAL4. However, it should be noted that this level can be weighted down by some errors arising from the lack of the data about the tools used by specialized CC laboratories. In addition, an influence on the final level of attack potential and the strength of security function arises not from the security mechanisms (identified as moderate), but only from the inconsistency of their documentation with CC requirements.

Tab. 4. Evaluation Assurance Level for CA network exemplary
Tab. 4. Poziom uzasadnionego zaufania dla przykładowego sieciowego urzędu certyfikującego

Scenarios	Value of attack potential	SOF - Level	Evaluation Assurance Level
S1	7	Low	EAL 4
S2	8	Low	
S3	10	moderate	
S4	9	Low	
S5	10	moderate	

5. Conclusions

Presented investigations revealed that it is possible to perform detailed evaluation of the risk analysis in accordance with international standard (ISO/IEC -27001 and ISO/IEC 15408) with a minimal adaptation of MEHARI method. Moreover, the obtained results are identical to the evaluation results according to CC for considered system and confirm the usefulness and correctness of the elaborated approach.

The issue discussed in the paper is an interesting analytical problem in the field of security evaluation of IT systems. It is possible to continue further research to obtain better precision and formalization of the method to be more compliant with CC. In author's opinion the proposed approach will enable to evaluate the risk more precisely and enhance the evaluation assurance level to IT systems as discussed in section 3, and enable the cost reduction during adaptation of each system to CC requirements. In addition, such an approach should help the organizations in the evaluation and preparation of their systems, etc.

6. References

[1] PN-ISO/IEC - 27001: Information technology – Security techniques – Information security management systems — Requirements, 2005.
[2] ISO/IEC - 15408: Common Criteria for Information Technology Security Evaluation, version 3.0, Part 1: Introduction and general model, June 2005.
[3] PN-ISO/IEC-13335: Information technology – Guidelines for the management of IT Security – Part 1, Part 2, Part 3, 1996-1998.
[4] Federation of European Risk Management Associations "FERMA": Risk Management Standard, 2003.
[5] Common Criteria for Information Technology Security Evaluation, version 3.0, Part 2: Security functional requirements, June 2005.
[6] Common Criteria for Information Technology Security Evaluation, version 3.0, Part 3: Security Assurance Requirements, June 2005.
[7] Common Methodology for Information Technology Security Evaluation, version 3.0, July 2005.
[8] http://www.insight.co.uk/products/cramm.htm 2011.
[9] http://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=METHODES, 2011.
[10] Swiderki Frank: Threats modeling, MS Press, 2005.
[11] EU Directive 1999/93/EC of the European Parliament and the council of 13 December 1999 on a Community framework for electronic signatures.
[12] http://www.cesg.gov.uk/

otrzymano / received: 03.05.2011
przyjęto do druku / accepted: 06.06.2011 *artykuł recenzowany*