Trust construction for security functions and mechanisms of IT system using results of risk analysis

PhD Imed El FRAY
Graduated from the Department of Marine Technology, Szczecin University of Technology in 1993. In 1997 obtained PhD in the field of Marine Technology (specialty: Automatics and machine steering). Main research interests: risk analysis, trusted systems. Employed as Associate Professor at the Faculty of Computer Science and Information Technology, West Pomeranian University of Technology, Szczecin.

e-mail: iclefray@w.zut.edu.pl

Abstract

In this paper the new approach enabling trust construction for security functions and mechanisms of IT system is proposed. It is based on specific determinants of risk values and trust values and uses „MEHARI_V3” risk analysis method. The proposed approach takes into account functional requirements and a trust justification for security means defined in ISO/IEC 15408 standard as an extension for security domains determined in MEHARI method.

Keywords: Risk analysis, trust and security, PKI.

Budowa zaufania do funkcji i mechanizmów zabezpieczeń systemu IT na podstawie wyników analizy ryzyka

Streszczenie

W artykule zaproponowano nowe podejście umożliwiające budowę zaufania do funkcji i mechanizmów zabezpieczeń systemu IT na podstawie określonych determinantów wag ryzyka, z wykorzystaniem gotowych scenariuszy zawartych w bazie wiedzy na zasadzie licencji GNU „Mehari V3” oraz wartości zaufania z wykorzystaniem wymagań na funkcjonalne zabezpieczenia zawartych w części drugiej normy pt. „Kryteria oceny zabezpieczeń teleinformatyki” i wymagań na uzasadnienie zaufania do zabezpieczenia z części trzeciej cytowanej wyżej normy. Proponowane podejście wykorzystuje nowo powstałą tabulę awersji poziomu zaufania do systemu w zależności od czynników określających determinanty wartości zaufania i wag ryzyka. Tabela awersji poziomu zaufania jest oparta na tablicach awersji ryzyka zawartej w metodzie Mehari. Wartości determinantów wag ryzyka, wartości zaufania oraz poziomu zaufania określone są doświadczalnie na podstawie wykonanych analiz ryzyka oraz opracowanych profilów zabezpieczeń systemów dla różnych instytucji. Proponowane podejście łączy w sobie zalety dwóch norm związanych z analizą ryzyka ISO/IEC 27001 i oceną bezpieczeństwa systemów ISO/IEC 15408 oraz umożliwia zwiększenie dokładności procesu szacowania ryzyka i zwiększa poziom zaufania odbiorców systemów IT.

Słowa kluczowe: Analiza ryzyka, bezpieczeństwo i zaufanie, infrastruktura klucza publicznego.

1. Introduction

There are different threats for an information stored in IT systems; it is endangered by unauthorized disclosures, modifications and destructions. Those threats can be invoked by faulty activity of the system and due to the other reasons as well (e.g. negligence, defects and attacks against IT system). This situation invokes the fundamental question for users of IT systems: can information be entrusted to the given system? The positive answer confirms trustworthiness of the system and is equivalent to an acceptance of risk for information assets in that system.

A. Josang demonstrated in „An Algebra for Assessing Trust in Certification Chains” [1] that assurance levels can be calculated on the base of positive answers and negative experiences.

P. Herrmann in "How to Integrate Trust Management into a Risk Analysis Process” [2] integrated the definition of an assurance level proposed by A. Josang with an audit process. He demonstrated that “As higher the trust in the good-naturedness of the involved parties is, as lower the likelihood will be assumed”. In consequence, the risk level will also decrease if the trust in the involved parties is high.

The new approach is proposed on the base of the statement concerning the dependence of an assurance level on a risk level. It determines the assurance level of IT system according to results of risk analysis. There an assurance level of a given system depends on factors specifying determinants of risk and trust values.

2. Description of risk analysis method

The crucial element of a risk analysis method is the way the risk is identified. An approach to this identification has to be a methodical one, to guarantee the consideration of all organizational activity areas and related risks as well [3].

Up to date over a dozen or so methods supporting a risk analysis process have been developed. The most of them, e.g. CRAMM [4], COBRA [5], etc., are commercial ones and are widely used by various organizations. These methods are based on standards ISO/IEC-27002 [6] and ISO/IEC-27001 [7] mainly.

For the purpose of this paper „MEHARI_V3” method [8] has been chosen. In comparison with the other ones mentioned it is available widely on the base of GNU license, it is usually used in various organizations (it is the successor of MARION method [9] developed for French banking association and widely used in banking systems) and is compliant with standards and recommendations stated above.

The structure of MEHARI risk analysis method (Figure 1) is similar to the structures of CRAMM and COBRA methods; it applies the knowledge concerning identification and value assessment of assets, threats levels and vulnerabilities evaluation.

Fig. 1. The structure of „Mehari V3” risk analysis method

Rys. 1. Prezentacja Metody analizy ryzyka „Mehari V3”
It is shown on the Figure above that risks are assessed concerning two values obtained from a risk analysis:

- **impact values** – it is the function of assets values (resulting from classification) and results of actions reducing an influence of threats on assets related to each security criteria (availability, integrity and confidentiality),

- **potentials of threats** – dependent only on an efficiency of planned actions and related to a given asset’s environment for example (natural, erroneously generated or generated by an adversary).

Both values are calculated on the base of the scenario set included in „MEHARI V3 Knowledge bases [9]” and consisting of threats for an organization’s IT system functionality.

Each of the scenarios (illegal disclosure, distribution or making data accessible, data manipulation, lost of data sets, etc.) considers some actions determining impacts and potentialities. Any of these actions is itself the set of problems (criteria) considering factors which can invoke a specific assessment of system sensitivity, efficiency of implemented security mechanisms (e.g. access control mechanisms), organizational procedures, etc. This assessment has to be the objective one and to be focused on a current situation in the particular and well defined area of a given security domain.

Evaluation methods and algorithms for particular actions, effects, impacts and assets’ classification are available e.g. in [8, 9, 10]. In this paper the final risk evaluation on the base of the risk aversion table is presented (see: Table 1).

### 3. Trust construction for security functions and mechanisms of a system

The trust construction for security functions and mechanisms of IT system can be performed ordering the evaluation of its security means in expensive specialized accredited laboratories, e.g. [11, 12]. Such an evaluation is done on the base of Common Criteria (ISO/IEC 15408 [13, 14, 15, 16]), due to their important role for decision makers deciding about a risk acceptance when assets are placed in a threatened environment.

Common Criteria were developed to make systems and applications compliant with world-wide accepted standards. The idea of that standard is to create one common scheme of evaluation for particular IT security technologies [15]. However R. Anderson has pointed disadvantages of these schemes in [17], e.g.:

- it is assumed the well trained and obedient personnel (accredited by appropriate state security services) is employed in laboratories evaluating and issuing certificates,
- they do not consider administrative security means, nor physical and technical ones (e.g. emission security and cryptographic algorithms),
- the trustworthiness of certification can be doubtful because it is based on the trust in state governments which supervise certification bodies activity, etc.

Even if mentioned above disadvantages are known, the great advantage of Common Criteria is that they offer functions, criteria, etc., which should be taken into account during processes of a design, redesign and evaluation of new or modified systems. They can also serve as an efficient tool to trace various threats and to consider these threats as factors deciding about resistance of an evaluated system against various attacks.

A negligence of administrative, physical and technical aspects in the case of security elements, that was stated as a serious defect in [17], becomes an advantage making an evaluation possible without relation to functional and operational environment of a system in question. It makes possible to perform a risk analysis according to common evaluation schemes and related methodologies and without considering selected elements of an external environment.

Using above mentioned possibilities and performing the standard risk analysis for other phases (taking into account selected elements of an external environment), some new proposal is defined. This new approach could be an alternative for expensive specialized laboratories, and could encourage managers, auditors and other to consider its functions, mechanisms, criteria, procedures, etc., in a practical risk analysis of systems in any phase of design process and during an issuance of declarations concerning the security of products introduced into the market, especially when law regulations enforce to do it.

### 4. Description of proposed approach

Usually the trustworthiness of IT systems is stated on the base of identified risks. Unfortunately, such an approach does not ensure the all reasons of greater risk are identified; therefore an influence of some system elements can be evaluated inappropriately. The way to avoid this situation is to consider the trust to existing system elements. The following elements can be taken into account:

- properly acting and implemented functional components with well grounded trust on the base of Common Criteria’s parts 2nd and 3rd; these components are relevant for an implementation of assumed security targets, requirements fulfilled during their design and creation and an analysis of results of potential security means’ vulnerabilities;
- correctly and appropriately performed actions assigned to the users, properly installed and configured hardware and software, a correct management, etc., all of them relevant as
countermeasures for identified threats and related vulnerabilities of assets. It is essential that the elements mentioned above can be considered together during the evaluation of the system and in the risk analysis process as well. However, it should be emphasized that during the evaluation of the system the first of above items is particularly analyzed, and the second one is omitted (they do not consider administrative, physical and technical security aspects; see: chapter 3 of this paper). In contrary, in the case of the risk analysis the first item is ignored and the analysis is focused mainly on the environment, the management and the way the user treats system actions and procedures being in force (it is assumed the most of functional components work properly, they are trusted - i.e. with the relevant assurance level, there are an appropriate documentation for them and they are tested).

The idea of a new proposed approach is the mapping of both elements mentioned above (the evaluation and the risk analysis of the system). It is based on MEHARI method extension with additional modules of functional and assurance requirements for the system according to Common Criteria (Figure 2).

![Diagram of functional and assurance requirements module as an extension of Meheri method](image)

**Fig. 2.** Functional and assurance requirements module as an extension of Meheri method

Rys. 2. Moduł wymagań funkcjonalności i uzasadnienia zaufania do systemu jako rozszerzenie metody Meheri

As it is shown on Figure 2, Common Criteria divide security requirements into separated categories - functional and concerning an assurance.

Functional requirements are defined for system functions intended for IT security means’ implementation. These requirements specify desirable performance of security functions and mechanisms. They include e.g. requirements for identification, authentication, security audit and non-repudiation of origin.

Assurance requirements are specified for software and hardware designer’s activities (activities of the Developer) specified in Common Criteria) and documentation. The examples are rigorous requirements for a production process, delivery, installation and start up of hardware and software components, support, etc.; they include also requirements concerning an identification and analysis of security means’ potential vulnerabilities.

Both types of requirements (functional and concerning an assurance level of the system) include an enumeration of relevant components, families and classes. Components of classes concerning identification, authentication, rigorous requirements for design processes, etc., are assigned to action determined in MEHARI extended metod (Figure 2). These components take into account all criteria which have to be met by security functions and mechanisms to obtain required EAL value.

Finally, according to stated above requirements, criteria, etc., the way the trust level of a given system is assessed and mapped in Table 2 relevant for MEHARI method:

<table>
<thead>
<tr>
<th>Determinants of trust value</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>Trust level (calculated along diagonals)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 (positive trust)</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>Unreliable</td>
</tr>
<tr>
<td>2 (moderate trust)</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>Untrusted</td>
</tr>
<tr>
<td>3 (neutral trust)</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td>Trusted</td>
</tr>
<tr>
<td>4 (negative trust)</td>
<td>3</td>
<td>3</td>
<td>4</td>
<td>4</td>
<td></td>
</tr>
</tbody>
</table>

The table presents that the assurance level is determined by two determinants:

- **Determinants of risk value** – dependent mostly on risk values for scenarios with the greatest importance for an organization, and
- **Determinants of trust value** – dependent on requirements relevant for IT security measures, i.e. functional and assurance requirements assigned to particular action presented on Figure 2.

For the purpose of the new approach, especially due to its large range, the whole work consists of two parts. The first one introduces for the first time Table 2 presented above. Additionally the scale of trust is created. It is based on determinants of risk and trust values used above and includes an explanation for each position from this scale. The second part of this work is an example of the new method implementation in the case of the real PKI Certification Authority involved in management and servicing of public key certificates (and it is not presented in this paper).

### 4.1. Determinants of risk value

For every critical process from an analyzed system the risk value is calculated separately according to MEHARI method; it is performed for any scenario presented in Table 1. However, because the security of the system depends on each identified scenario, it is impossible practically to indicate more or less significant one. On the other hand, from the theoretical point of view, the scale of determinants of risk value for the whole of the system can depend on these scenario values (see: Table 1) which have assigned the most significant meaning for an organization in question (such a scenario can destabilize the system functionality), and the other scenarios with the worst results (not permissible or not accepted).

The scale of determinants of risk value is presented below:

- **R=1 – insignificant**: this value is assigned to the system when calculated risk values for scenarios with the greatest importance for a given organization do not exceed 1; for other scenarios this value can be 1 or 2,
- **R=2 – serious**: this value is assigned to the system when calculated risk values for any scenario do not exceed 2,
\[ R=3 \text{ – very serious: this value is assigned to the system when calculated risk values for scenarios with greatest importance for a given organization do not exceed 2; for other scenarios this value can be between 1 and 3,} \]

\[ R=4 \text{ – vital: this value is assigned to the system not meeting requirements relevant for } R=1, R=2 \text{ and } R=3. \]

### 4.2. Determinants of trust value

Determinants of trust value will be defined on the base of functional components and assurance to the system in question taken from 2\(^{nd}\) and 3\(^{rd}\) parts of Common Criteria. Determinants for functional components are grouped according to differentiated levels of security (for example the following criteria have been introduced: weaker or stronger restrictions, rigorous actions/evidences, automated mechanisms used, etc.), and EAL from Common Criteria [16] are considered in the case of assurance components, particularly taking into account documentation for tools used (e.g. tools for configuration management, testing, etc.) and security functions and mechanisms.

The proprietary created scale for determinants of trust value is presented below and it is relevant for any analyzed system or group of IT systems:

\[ D=4 \text{ – negative trust: on this level functional components of the analysed IT system ensure a correct operation in the basic security range. Functional and assurance components are as follows:} \]

- Functional components, including security mechanisms, enable:
  - data enciphering and deciphering,
  - access control, confidentiality protection and integrity of users data,
  - users authentication and identification before any action in the system,
  - separation of management domains and roles in the system.
- Assurance components, including documentation, ensure:
  - corectness of hardware and software operation,
  - hardware and software accordance with operation documentation, including procedures of secure delivery, installation and start-up, and operational tests results for particular modules (the required test documentation should be prepared by an institution independent from hardware and software developer).

\[ D=3 \text{ – neutral trust: it is necessary to meet by functional and assurance components all requirements specific for } D=4, \text{ and additionally the following:} \]

- Functional components, including security mechanisms, enable:
  - Generation, review and analysis of security audit data,
  - data authentication,
  - integrity of data stored in a system,
  - administration of system configuration parameters,
  - limitation for a number of working sessions,
  - limited authentication time period.
- Assurance components, including documentation, ensure:
  - description of functional specification and a specification of security functions interfaces,
  - detailed reports/evidences (prepared by hardware and software supplier) from basic tests, security functions strength analysis and looking for evident vulnerabilities,

\[ D=2 \text{ – moderate trust: it is necessary to meet by functional and assurance components all requirements specific for } D=4 \text{ and } D=3, \text{ and additionally the following:} \]

- Functional components, including security mechanisms, enable:
  - secure storage of events, causes and traces of a security audit,
  - non-repudiation of data source and receipt,
  - cryptographic keys management,
  - data export and import to/from protected zones,
  - data transfer control inside the system,
  - maintenance of authentication errors,
  - trusted time stamping.
- Assurance components ensure documentation of:
  - configuration management process, including all applied procedures of version and changes management for hardware and software used in an organization in question,
  - control mechanisms and security procedures implemented in a development environment (i.e. hardware and software are not penetrated during a development phase),
  - detailed reports/evidences concerning requirements resulting from a better test covering of security functions and mechanisms and/or procedures for hardware and software.

\[ D=1 \text{ – positive trust: it is necessary to meet by functional and assurance components all requirements specific for } D=4, D=3 \text{ and } D=2, \text{ and additionally the following:} \]

- Functional components, including security mechanisms, enable:
  - performance of a selective security audit,
  - protection of returned data after an authentication,
  - expiration of attributes validities after a determined time period,
  - session blocking and exit.
- Assurance components ensure documentation of:
  - description of projects and implementation presentations for hardware and software,
  - detailed reports from an independent vulnerabilities assessment and analysis (i.e. confirmation of the resistance against penetrating attacks performed by skilled attackers).

### 4.3. Assurance level

System assurance levels presented in Table 2 are defined with the following assurance scale:

- **Trusted**: it means the system is secure and the system and its services can be treated as trusted. The trust concerns all security aspects, including the storage and processing of sensitive data, and management and access control with the usage of the strongest cryptographic mechanisms. The system is well designed, correctly installed, configured, tested, operated and managed. It guarantees all anxious signals will be recognized timely and relevant countermeasures will be used. All abusement trials will be detected in a reasonable time and a compromising will not occur.

- **Untrusted**: it means the system is equipped with some security means, but they are insufficient. Sensitive assets should not be entrusted to it until the higher assurance level is reached. It can be the matter of security means built-in and external ones as well (i.e. external environment).

- **Unreliable**: it is not possible to ensure the security of assets. Such a system should be completely rebuilt. The system and its environment are not secure.

### 4.4. Justification of assurance levels

If D-value diminishes a number of used security mechanisms increases, therefore an impact of other factors is less, especially of those concerning the human factor. More requirements concerning security functionalities, more hermetic and resistant system. It becomes more resistant against threats, manipulations, etc. The
following examples make this thesis reliable:

- Automatic threat detection, information and reaction reduce the probability of effective attacks and enforce an immediate control of incidents and relevant interventions,
- Detailed logs of system events and availability of diagnostic tools enable an easy interpretation of logs and detection of potential threats and persons responsible for them,
- Correctly configured unstable states detection system and an automatic recovery system enable to react immediately to restore a stable state of IT system,
- System users activities control based on a profiles concept and a rigorous authorization policy make a system resistant against voluntary incidental abusesments and potential conscious acts of users’ wrong will as well,
- Protection of information concerning alarm and system configuration conditions increases the user activities control and enforces their proper behaviour,
- Protection from known forms of attacks reduces an attacker’s force and determination suitable for breaking system security measures,
- Total control of all forms of information storage protects from an incidental data disclosure to unauthorized persons.

Under such an assumption the second factor from Table 2 (determinant of risk value R) has a different meaning for different values of D:

- D=4: this case indicates the situation when security and control functions and mechanisms are insufficient. Possible greater values of R depend on other factors (physical security of the system and a human factor). For this case the following principle should be accepted: the higher physical security level and independence from personnel – the lower risk value.

The main limitation are components used because they do not ensure complete protection. An illogical satisfying assurance level to the system can be obtained when the lack of security functions and mechanisms is replaced by fast and accurate human actions. However, this level is limited and burdened by the constant risk (e.g. due to attacker penetrations) - in every moment the system can become untrusted or even unreliable,

- D=3: the situation is similar to the previous one (D=4), but components used ensure the higher security level of the system due to the usage of additional management elements and controls. It should be underlined that in this case the assurance level of the system is not burdened by the constant risk, nevertheless it requires permanent monitoring measures and changes in the system,

- D=2: in this case the system has the most of security functions (mainly management facilities). Such a system is able to counteract against the most of known medium force attacks (and it is the fact the most of existing attacks are such ones). It ensures also the higher stability due to the restricted control of data inputs and configuration changes.

If the threat indicated by the risk analysis is small (it can be the result of personnel’s engagement and the relevant physical security measures as well), eventual flaws in functional components can be completely compensated and the system is trusted. If the risk indicated by the risk analysis is high or very high then the situation is completely different. To obtain a satisfying assurance level in the system all threats resulting from environmental and human factors should be eliminated. If it is not the case then the system is untrusted one,

- D=1: due to the usage of all mentioned above security functions and mechanisms the system ensures the maximal security. The system can be treated as trusted, even if some moderate risks exist. If the risk analysis indicates a high or very high risk then obtaining the relevant assurance level requires only monitoring of an organization and training/controlling of personnel.

5. Conclusions

The presented approach is the trial to combine advantages of ISO/IEC 27001 and ISO/IEC 15408 standards. This approach requires to extend „Mehari V3” risk analysis method, particularly in security domains directly associated with supplied hardware and software. The extended method would consider all security functions and mechanisms, together with relevant documentation, in such a manner that all known objections (stated for example in [17]) could be eliminated.

The questions discussed in this paper are particularly interesting research problems from the IT security assessment point of view. The next steps of presented work will be focused on more detailed and formal description of the presented approach, including direct links to relevant Evaluation Assurance Levels (EALs) defined in Common Criteria.

The author believes the proposed method will enable to increase the precision of the risk assessment process, and consequently will make an assurance level of IT systems higher.

6. References


Artykuł recenzowany