Effective Design of Trusted Information Systems

Ludek Novák
novak@isaca.cz

Information Systems Audit and Control Association
Czech Republic Chapter – ISACA CRC
Národní trída 9
110 00 Prague, Czech Republic

Abstract

This article describes an advanced approach to a security design of up-to-date information systems and basic actions that are necessary for effective and accurate covering of all reasonable security necessities. The expressed methodology is based on a draft of the new standard ISO/IEC PDTR 15446, which is mostly designed to formulate Common Criteria's Protection Profiles or Security Targets. But recommended procedures and measures are often usable for the effective security design of trusted systems in general.

The design starts with a general description of a purpose and boundary of an information system. A formation of the security design begins with a description of a security environment. The next step is identification and specification of the security objectives. Selecting an appropriate set of security requirements is a way to meet all the security objectives. The last step in the design is to observe a rationale of the objectives and the requirements.

This approach has been used for the security design of several information systems. The results of the security solution are clear, easy understandable, and very effective. So, this is the main benefit of the method. Another advantage is a close connection to the well-known Common Criteria Project and all its outputs.

Keywords: trusted information system, target of evaluation, security design, Common Criteria, security needs, security objectives, security requirements.

1. Introduction

This article describes an advanced approach to the security design of up-to-date information systems and basic actions that are necessary for effective and accurate covering of all reasonable security demands. The methodology rigorously states a security topic for given systems or products known as the target of evaluation. The *Target of Evaluation* (TOE) is an IT product or system and its associated administrator and user guidance documentation that is the subject of an evaluation.

The term TOE is closely connected with the security evaluation and a related methodology. But the term TOE is likewise commonly used in the article not matter if we are going to a process of any formal evaluation. Any necessity cannot be there to evaluate our system, but a tight relationship with the evaluation procedures is always useful. In addition, standardised evaluation procedures may bring a good practice to our design work.

The method rises from [1] and its structure includes five principal steps. The design starts with a general description of a system that is a subject of the design. The security design contains a description of a security environment, a creation of the security objectives and a selection of the security requirements. The last step is an observation of a rationale of the objectives and the requirements. The structure is shown on Figure 1 and the individual steps are explained in the following text.

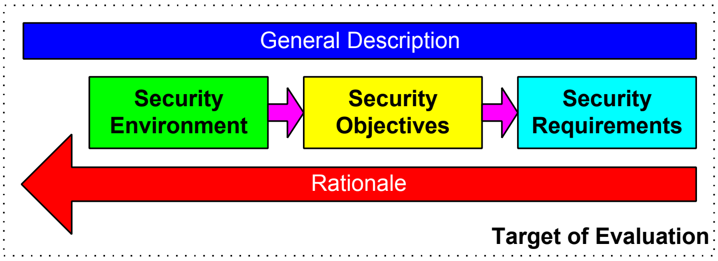

Figure 1. Structure of the TOE design

All the needs, the objectives, and the requirements should be uniquely labelled for a simple reference. There are two possible options for this. The first one is sequential numbering of all labels e.g. A.1, R.2, P.3, O.4 etc. This approach is difficult to manage, but sometimes it is useful. The second option is a label providing a meaningful name or an abbreviation e.g. T.ACCESS, TA.USER, OE.INSTALL, F.PHY.UPS etc. This way is recommended because it is more memorable. Label examples are shown in Annex A.

2. General Description

The whole process of the effective security design starts with a good understanding, what the TOE really is and what is its purpose. The *General Description* provides background information to the TOE and serves as an aid to an appreciation of its security requirements and intended usage. This aspect is not directly connected with the security design, but clear understanding of the TOE purpose, including its functions and usage, is a vital necessity of a well-behaved security development. The general description can be divided into the following four main sections:

1. *Document identification* – includes a name of the document, a history of its version, a list of authors, a date and a body which approved it, etc.
2. *General TOE functionality* – is a collection of information on the TOE that is relevant to the TOE operation and running. It is quite easier to understand the TOE security behaviour if you have a general knowledge about the functional purpose of the TOE.
3. *TOE boundary* – tells what the TOE is and what it is not. The TOE boundary must be defined in a physical way (hardware and/or software components/modules) and in a logical way (functional and security features offered by the TOE).
4. *TOE operational environment* – is a high level explanation, where the TOE is used, covering important assumptions, business constrains, and other key elements.

The general description is presented by a common language as well as by some technical pictures, which show a structure and other details of the TOE.

3. Security Environment

The first step of the security design is a description of the TOE security background. The *Security Environment* provides a definition of the context in which the TOE resides and explains the nature and the scope of the security needs to be addressed by the TOE. This description specifies assumptions defining the limits of the security conditions, identified threats to the assets requiring a protection together with a description of the assets and threat agents, and any organisational security policies with which the TOE must comply. A relationship is shown on Figure 2.

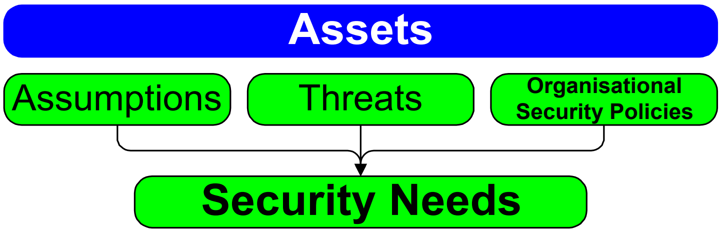

Figure 2. Definition of Security Needs

The goal of the environment specification is to avoid any disordered discussion if the TOE meets all the security needs. It helps to focus reader's attention on what the important aspects of security are. It is useful to specify all the security needs at the same level of details. Therefore, it is simpler to avoid overlaps and gaps among different needs. This makes it easier to prevent the potential confusions of the security environment understanding as well as to simplify the rationale by avoiding repetitions.

3.1 Assets

An *Asset* is an information or a resource, which needs to be protected by countermeasures of the TOE. A goal of a description of assets is to recognise what the assets that require protection are. A designer should concentrate on the assets, which have a primary value for an organisation (e.g. financial value, level of reputation, etc.). All the assets must be distinguished and briefly described. In addition, it is useful to establish an owner who is responsible for each asset. A label of any asset starts with a letter R abbreviates Resource, e.g. R.DATA.

3.2 Assumptions

An *Assumption* is a potential threat to an asset and this threat is not relevant to or involved in the TOE security. The assumptions should include aspects relating to the intended usage of the TOE and its environmental (e.g. physical) protection. Other assumptions are connectivity aspects (e.g. a firewall must protect all connections between a private network and a hostile one) or personnel aspects (e.g. expected skills and knowledge of users) etc. For the design, it is important that all formally identified assumptions have to be upheld by the security objectives. A label of any assumption starts with a letter A abbreviates Assumption, e.g. A.PEER.

3.3 Threats

A *Threat* is an undesirable event, which is characterised in terms of a threat agent, a presumed attack method, any vulnerability and an identification of the assets under an attack. The treat definition can be solely omitted if the security needs are fully defined by the assumptions and by the organisation security policies. In practice, it is recommended to include a statement of the threats, which provides a better understanding of the needs, into the design. The threats are more closely connected to the TOE too. It means the threats are more actual, flexible and up-to-date than the other kinds of the needs are. A label of any threat starts with a letter T abbreviates Treat, e.g. T.ACCESS.

For completeness, there are threats not directly addressed by the TOE, like physical attacks, abuse of trust by privileged users, improper administration, etc. These threats are addressed by the objectives for the environment. A label starts with letters TE abbreviate Threat Environment, e.g. TE.CRASH.

A *Threat Agent* may either be human or non-human, although in the domain of security, greater attention is usually given to those threats that are related to malicious or other human activities. A label of any threat agent starts with letters TA abbreviates Threat Agent, e.g. TA.USER.

3.4 Organisational Security Policies

An *Organisational Security Policy* is defined as one or more rules, procedures, and practices imposed by an organisation or by other authorities. It is appropriate to specify the OSPs where the TOE must comply with some special set of rules (e.g. protection of classified information). The OSPs may be omitted if the security needs are fully defined by the treats. A label of any organisational security policy starts with a letter P abbreviates Policy, e.g. P.MAC.

4. Security Objectives

The next design step is identification and specification of the *Security Objectives*. It provides a concise statement of the intended response to the security needs in terms of the security objectives to be satisfied both by the TOE and by IT and non-IT measures within the TOE environment. For that reason, we recognise two types of the objectives: objectives for information technology and objectives for the environment (see Figure 3).

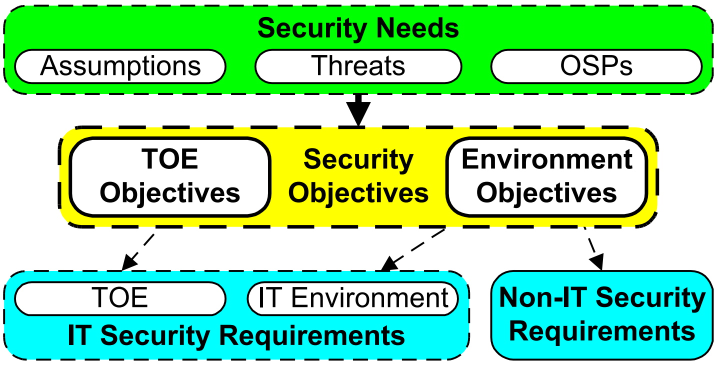

Figure 3. Role of Security Objectives

4.1 Security Objectives for TOE

The *Security Objectives for the TOE* must express what the responsibility of the TOE and its security functions is. The significance of the security objectives is to realise the extent of the security considerations addressed directly by the TOE. A label of any security objective for the TOE starts with a letter O abbreviates Objective, e.g. O.A&I.

All the security objectives for the TOE have to be fully satisfied by technical (IT) countermeasures. Three general types of security objectives can be identified:

1. *Preventative Objectives* which prevent a threat from being carried out, or limit ways in which a threat can be carried out (e.g. user identification and authentication – O.I&A);
2. *Detective Objectives* which provide means to detect and to monitor an occurrence of events relevant to the secure operations of the TOE (e.g. proof of origin – O.NOREPUD);
3. *Corrective Objectives* which require the TOE to take actions in response to potential security violation or other undesirable events in order to preserve or return to a secure state and/or limit any caused damage (e.g. data recovery – O.ROLLBACK).

4.2 Security Objectives for Environment

The *Security Objectives for the Environment* have to be identified to address those aspects of the security needs that the TOE will not or cannot be expected to do. These objectives are to be satisfied by either technical measures implemented in the IT environment or by non-IT (e.g. procedural) measures. A label of any security objective for environment starts with letters OE abbreviates Objective Environment, e.g. OE.PHYSICAL.

5. Security Requirements

Selecting an appropriate set of security requirements is a way to meet all the security objectives. The *Security Requirements* define the security functional requirements on the TOE, the security assurance requirements, and any security requirements on software, firmware and/or hardware in the IT environment for the TOE. The IT security requirements are to be defined by using a functional and an assurance component from ISO/IEC 15408 [3] or [4] (see Figure 4). The use of other source is possible as well.

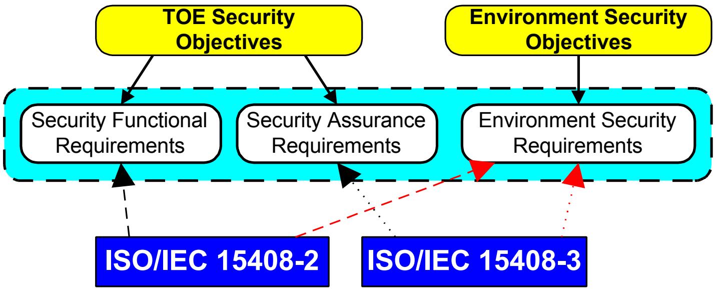
TOE Security Objectives
Environment Security Objectives
Security Functional Requirements
Security Assurance Requirements
Environment Security Requirements
ISO/IEC 15408-2
ISO/IEC 15408-3

Figure 4. Derivation of Security Requirements

It is important to keep an excellent overview over the whole system of all the security requirements. Effective grouping of requirements, which are focused on covering the similar security features, is a good way to solve this. A dependency among security components within the TOE is another issue. This means there can be a requirement, which cannot work without the other one. In this case, the former satisfies the objective directly. The latter provides the support for the former and satisfies the objective indirectly.

It is very effective to use a certified Protection Profile, which has been developed and evaluated by someone else, to formulate a complex of the requirements. The formal and standardised methodology offers this possibility and makes the sharing of information security know-how around the world simpler.

5.1 Security Functional Requirements

The *Security Functional Requirements* (SFRs) on the TOE identify demands for the security functions, which the TOE must provide to fulfil the security objectives for the TOE. The requirements can be concentrated on more general security functions what are better for high-level designs. There are seven groups of the security functions recommended by [1]:

1. *Identification and Authentication* – all safeguards address the requirements for functions to establish and to verify a claimed user identity and to set up a session. A label starts with F.IA.
2. *Access Control* – all safeguards restrict an access to the system resources, networks, computers, applications, files, and programs. A label starts with F.AC.
3. *Audit* – all safeguards involve recognising, recording, storing and analysing information related to the security relevant activities. A label starts with F.AU.
4. *Integrity* – all safeguards protect unauthorised modification of information and keep data and system consistency. A label starts with F.IN.
5. *Availability* – all safeguards take care of accessibility of system services and required resources, such as processing and/or storage capability. A label starts with F.AV.

6. *Privacy* – all safeguards provide a user protection against discovery and misuse of identity by other users. A label starts with F.PR.
7. *Data Exchange* – all safeguards authenticate communication sites and protect the integrity and confidentiality of exchanged data. A label starts with F.EX.

The other way is associated with the requirements for a complex structure of the security functions presented in [3]. This approach is more technical and gives attention to the security mechanisms. As a result, such way is more adequate to low-level designs, especially security product designs.

5.2 Security Assurance Requirements

The *Security Assurance Requirements* (SARs) on the TOE prescribes clear objective criteria, which express quality of the development. The requirements set up demands for the developer actions, for content and presentation of evidence, and for independent control activities (e.g. evaluation, accreditation) etc.

The selection of the demands may be relatively straightforward if you can select a predefined assurance package. There is a hierarchically ordered set of seven packages in [4] that are called the Evaluation Assurance Levels. It is broadly recommended to use one of these packages to formulate a base of the assurance requirements.

5.3 Security Requirements on the Environment

The *Security Requirements on the Environment* (SREs) brings up the claims which would not be under a direct control of any IT security function within the TOE[5]. These requests express the demands on coordination between the security functional and assurance requirements and associated management techniques that need to be reliably propagated into the operation of the TOE and into recommendations for their utilisation. There are three main areas of the environmental requirements:

1. *Personnel Security* – all safeguards reduce the security risks resulting from errors or intentional or unintentional breaking of the security rules by personnel. A label starts with FE.PER.
2. *Physical Security* – all safeguards deal with a physical protection and are applied to buildings, secure areas, computer rooms and officers. A label starts with FE.PHY.
3. *Procedural Security* – all safeguards aim at all procedures maintaining the secure, correct and reliable functioning of the IT equipment and related systems. A label starts with FE.PRC.

The security requirements on the IT environment are not standardised around the world. But there are a lot of national based standards, which are in close connection with the national security rules flowing from the law and regulations specifics. The Protection of Classified Information Act and its legal regulations, which are maintained by the National Security Authority [7], is a good example for the Czech Republic.

6. Rationale

The final step of the security design is a rationale. The purpose of the *Rationale* is to demonstrate that the designed TOE would provide an effective set of IT security safeguards and countermeasures within the TOE and its security environment. The rationale shows that the objectives are suitable to cover all aspects of the TOE security that is represented by the security needs. Consequently, it shows that the IT security requirements are suitable to meet the security objectives. Figure 5 illustrates the key aspects of the rationale.

[5] There can also be required a dependency on an underlying information technology, which is not a part of the TOE.

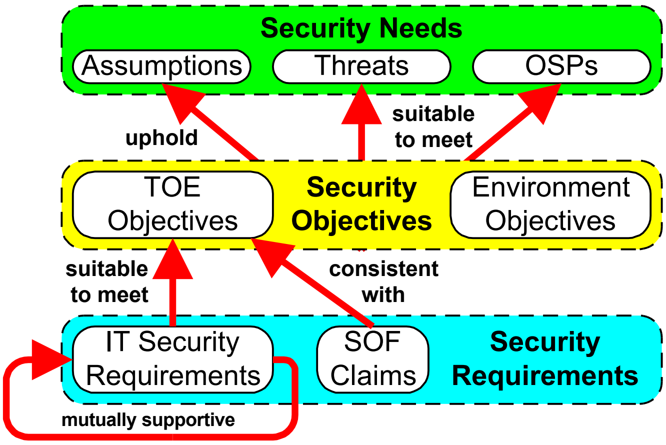

Figure 5. Rationale of Objectives and Requirements

6.1 Security Objectives Rationale

The *Security Objectives Rationale* demonstrates that the identified security objectives are suitable to cover all aspects of the security needs as they are specified. There are two steps. Firstly, you need to apply suitable means (like a cross-reference table or other methods) to show that each threat, organisational security policy, and assumption is addressed by at least one security objective and vice versa. This step shows that each object is necessary.

Secondly you should demonstrate that the objectives are sufficient to meet the needs. You provide informal arguments to supplement the table. The arguments must confirm that the objectives are right and proper to cover the needs. This step demonstrates the adequacy of the objectives.

6.2 Security Requirements Rationale

The *Security Requirements Rationale* makes evident the identified security requirements are suitable to meet the identified security objectives. You need to show that the requirements are both necessary and sufficient. Techniques to do this are the same like for the security objectives rationale. Furthermore, there must be arguments that explain reasonability of the assurance requirements, suggested Strength of Function (SOF) claims, and mutual dependencies among the requirements.

7. Conclusions

This approach has been used for the security design of several information systems. Results of the security solution are clear, easy understandable, transparent, and very effective. So, this is a main benefit of the method. The whole methodology follows the new security methods based on the well-known Common Criteria Project and all its outputs. Another advantage is a possibility to create a general know-how that can be easily shared among security experts inside as well as outside any organisation.

Semiformal method is quite more effective than informal one. The principal benefit is that semiformal output can be reused for similar systems. This reduces development costs and cuts down the workload of involved security experts. In addition, the semiformal description effectively helps to adapt suitable former designs to the new situations.

8. References

[1] Information technology – Security techniques – Guide for the production of protection profiles and security targets, ISO/IEC PDTR 15446, ISO/IEC 2000.

[2] Information technology – Security techniques – Evaluation criteria for IT security: Introduction and general model, ISO/IEC 15408-1, ISO/IEC 1999.

[3] Information technology – Security techniques – Evaluation criteria for IT security: Security functional requirements, ISO/IEC 15408-2, ISO/IEC 1999.

[4] Information technology – Security techniques – Evaluation criteria for IT security: Security assurance requirements, ISO/IEC 15408-3, ISO/IEC 1999.

[5] Hanácek, P., Staudek, J.: Bezpecnost informacních systému: Metodická prírucka zabezpecení produktu a systému budovaných na bázi informacních technologií, ÚSIS, Praha, 2000.

[6] Purser, S.: Implementing Core IT Security Services, Proc. of 17th World Conference COMPSEC 2000, Elsevier 2000.

[7] National Security Authority's Web Pages, http://www.nbu.cz, NBÚ, Praha, 2001.

9. Annex A – Examples of Formal Labels

This annex includes examples of the labels and their meanings. A full list of the examples is a part of [1]. However, other lists, which are more dedicated to some kind of issues or which have closer association to national and/or further rules, may exist.

9.1 Security Environment

Assets

R.DATA Any data resource which is stored or maintained under control of the TOE.

R.SOFTWARE Any kind of software that the TOE consists of or that supports its running.

R.HARDWARE Any kind of hardware that the TOE consists of or that supports its running.

Assumptions

A.PEER Any systems with which the TOE communicates are assumed to be under the same management control and operate under the same security policy constraints.

A.PROTECT The TOE hardware and software critical to the security policy enforcement is assumed to be physically protected from any unauthorised modification by potentially hostile outsiders.

A.USER Users of the TOE are assumed to possess the necessary privileges to access the information managed by the TOE.

Threats

TA.CRASH A natural or another unpredictable event (e.g. fire, flood, failure etc.) which can influence or interrupt a correct operation of the TOE.

TA.USER Persons who are authorised users of the TOE.

T.ACCESS An authorised user of the TOE may access information or resources without having permission from the person who owns or is responsible for the information or the resources.

T.CAPTURE An attacker may eavesdrop on, or otherwise capture, data being transferred across a network.

TE.CRASH A human error or a failure of software, hardware, or power supplies may cause an abrupt interruption of the TOE operation, resulting in the loss or corruption of the security-critical data.

Organisational Security Policies

P.MAC The right to access information marked with a sensitivity designation is determined as follows:

An individual is only permitted to observe information if that individual is cleared to see it;

An individual must not downgrade the sensitivity designation of information, unless that individual has been given an explicit authorisation to perform such actions.

9.2 Security Objectives

O.I&A The TOE will uniquely identify all users and will authenticate the claimed identity before granting a user access to the TOE facilities.

O.MAC The TOE will protect the confidentiality of information. It is responsible for managing, in accordance with the P.MAC security policy, based directly on comparison between an individual’s clearance or authorisation for the information and the sensitivity designation of the information.

O.NOREPUD The TOE will provide a means of generating evidence that can be used to prevent that an originator/recipient of information could successfully deny sending/receiving that information.

O.PROTECT The TOE will protect itself against external interference or tampering by untrusted subjects or against attempts to bypass the TOE security functions by untrusted subjects.

O.ROLLBACK The TOE will provide the means of returning to a well-defined valid state by permitting a user to undo transactions in case of an incomplete series of transactions.

OE.PHYSICAL Subjects responsible for the TOE must ensure that those parts of the TOE that are critical to security enforcement are protected from physical attack, which might compromise IT security.

OE.INSTALL Subjects responsible for the TOE must ensure that the TOE is delivered, installed, managed, and operated in a manner that maintains IT security.

9.3 Security Requirements

F.IA.LOGON The TOE must identify and authenticate any user before granting any access to the TOE facilities.

F.AC.DAC The TOE must enforce defined access mode among subjects and objects that are under its control.

F.AU.REVIEW The TOE must be able to read recorded audit data and to interpret the information.

F.IN.DATA The TOE must protect data integrity and use appropriate mechanism for the detection of a loss of this integrity.

F.AV.SERVICE The TOE must assign a priority among each service and each subject in the TOE.

F.PR.ANONYM The TOE must provide its services without identifying user identity.

F.EX.SECRET The TOE communication service must protect confidentiality of any exchanged data by using an appropriate mechanism, e.g. encryption.

FE.PHY.UPS An uninterrupted power supply unit, with appropriate capacity, must safe the TOE running.

FE.PER.AWARE All TOE users must be aware of all security requirements and security rules.

FE.PRC.RIGHT There must be an appropriate procedure that has authorised a user to work with the TOE.