INFORMATYKA EKONOMICZNA BUSINESS INFORMATICS 3(29) • 2013
ISSN 1507-3858

Dariusz Rogowski
Institute of Innovative Technologies EMAG, Katowice
e-mail: drogowski@emag.pl

COMPUTER-AIDED TOOL BASED ON COMMON CRITERIA RELATED DESIGN PATTERNS

Abstract: The paper describes the results of an R&D project whose aim was to work out a computer tool supporting the development of IT products with built-in security features. The tool ensures that all security measures are applied into a product with regards to the requirements of the ISO/IEC 15408 standard (Common Criteria for Information Technology Security Evaluation). Nowadays there are only a few, limited solutions which support developers in using the Common Criteria methodology. The proposed tool supports three basic processes: security development, product development, and product evaluation as well as writing special evidence documents based on design patterns. Developers used the tool in software- and hardware projects and demonstrated it facilitates and speeds up the development processes of IT security-enhanced products.

Keywords: Common Criteria, security assurance, design patterns, computer-aided tool.

1. Introduction

Many developers of IT security-enhanced products wonder how to convince their clients that the security features embedded into the products are dependable and reliable. One of the ways is to engage a third party independent institution that can proceed with some of the evaluation and certification processes of the given product. Moreover, developers could use some standards, strict rules or requirements, methods and tools in order to prepare their products for successful assessment. To achieve this goal, both evaluators and developers can use the Common Criteria for Information Technology Security Evaluation standard (referred to as “Common Criteria” or “CC” throughout this paper). Common Criteria is an internationally recognizable standard ISO/IEC 15408 [*CC Part1…* 2012; *CC Part2…* 2012; *CC Part3…* 2012] to create assurance for an IT product. Such a product, according to CC terms, is called TOE – Target of Evaluation.

The standard provides a set of development rules and evaluation requirements described by a large number of assurance and functional components. Following these components is a very difficult, time-consuming and complex task. This is why some supporting documents and guidelines have been written. Many of them are issued by German Federal Office of Information Security (BSI) – the leader of research in the field of the CC standard. This guidance documentation gives some advice on the structure and contents of evidence documents. Some templates were issued and could be used by developers but still too much work has to be done on their own [Białas 2008; Rogowski, Nowak 2012].

Apart from help documentation, some supporting software tools were also worked out using the CC methodology. Unfortunately, these applications provided only basic functionality concerning only two documents (Security Target – ST and Protection Profile – PP), which describe the security specification of a product [Kane 2008; *International Common Criteria Conference* 2012]. Moreover, some of the software tools are not supported and developed by their producers any more. Although the solutions mentioned above were offered a few years ago, relatively little attention has been paid to other evidence documents needed for the evaluation process.

The guides and computer-aided tools are focused mainly on the preparation of STs and PPs documents. Apart from that, there is weak integration of the guidance knowledge within the software tools. In addition, if the developers want to create the evidence documents only by using the guidelines and templates, they still have a lot of work to do by themselves. They have to plan the structure of the document and find out what kind of information they should write down in the given section. That is why preparing the documentation is still difficult and not effective enough to encourage the developers to do this task. This problem has to be solved in order to make the whole development and evaluation processes cost-effective and developer-friendly.

The problem can be solved by a complete and integrated solution which was worked out in the CCMODE (Common Criteria compliant, Modular, Open IT security Development Environment) R&D project carried out by the Institute of Innovative Technologies EMAG. The aim of the project was to work out a methodology and tools to develop and manage development environments of IT security-enhanced products for the purposes of their future Common Criteria certification. As a result, a set of design patterns (the core of the methodology) was developed and then implemented in the computer-aided system CCMODE Tools. Thanks to the computer tool, developers receive one complete solution which facilitates the production processes of the TOE and related documentation.

The paper is organized as follows. Section II presents the state of the art. Section III explains the CC methodology used for working out the design patterns and their implementation into the computer tool. Section IV gives an overview of the CCMODE Tools main modules and their functionality used for evidence documents preparation. Section V contains some conclusions.

2. State of the art

The current version of Common Criteria, issued in 2012, consists of three parts. The first part is a general introduction to the CC methodology with an explanation of basic terms and definitions [*CC Part1…* 2012]. The second part describes security functional requirements (SFRs) which determine the desired security behavior of a TOE [*CC Part2…* 2012]. The third part, the most important for building the design patterns, defines the assurance requirements (SARs) for a TOE and evaluation criteria for PPs, STs and other evidence documents [*CC Part3…* 2012].

The results of CC-based evaluation are accepted in the 26 countries which joined the Common Criteria Recognition Arrangement (CCRA). Among these countries there is a group of Certificate Authorizing Members, which have implemented the standard and can carry out the evaluation and certification processes, and there is a group of Certificate Consuming Members which can only recognize already issued certificates. Poland does not belong to either of these groups. This arrangement allows end users to recognize certificates, regardless of the country in which they were issued. Therefore the certified products of different vendors can be easily compared and chosen by the users. To date, more than 2,100 IT products have been evaluated (including archived certified products).

So far, only one Polish product has been evaluated and certified according to Common Criteria. It is a secure signature creation device (SSCD) with key generation produced by the Polish Security Printing Works (pol. Polska Wytwórnia Papierów Wartościowych – PWPW) [*Certification Report…* 2012]. But in this case the evaluation and certification processes were carried out by German bodies according to their national evaluation scheme. There are some special military IT products which were accredited according to the old standard ITSEC (Information Technology Security Evaluation Criteria) [*ITSEC…* 1991]. But it does happen that some products have to consider the latest CC requirements during the accreditation processes. In these cases, both the developers and the Polish accreditation institutions like the Ministry of National Defense (pol. Ministerstwo Obrony Narodowej – MON) or/and the Internal Security Agency (pol. Agencja Bezpieczeństwa Wewnętrznego – ABW) must be prepared to use the Common Criteria standard in order to properly fulfill the accreditation procedures. These examples show that there is a need for the implementation of the CC standard in Poland and for the implementation of the CCMODE project results.

There are many other additional documents to the CC standard. One of them is the Common Evaluation Methodology (CEM) [*Common Methodology…* 2012] which helps evaluators to conduct the TOE assessment process. It defines the evaluation activities to be done by the evaluators and presents work units – the most granular level of evaluation work – that help to issue verdicts about the quality of the security implemented in the TOE. Other documents, like technical reports and users guides, explain step by step how to build evidence documentation. For instance, the ISO/IEC Technical Committee for Information Technology issued a technical report that is a guide for the production of PPs and STs [*ISO/IEC TR 15446…* 2009]. This report provides methodologies, techniques and practical tips that developers can use to prepare security specification documents in an efficient and consistent manner. BSI issued a guide for developers of the STs and PPs [*The PP/ST guide…* 2007]. Apart from that there is a guide that offers assistance to less experienced developers by extracting the information about the evidence from CC [*Guidelines for developer…* 2007]. It explains the requirements concerning the structure and contents of documents to be provided for the CC evaluation process. Another guide concerns the evaluation reports according to CC and gives some advice and recommendations on the structure of information provided in these reports [*Guidelines for evaluation…* 2010]. The CC standard and all the guides mentioned above are used by the developers in practice for writing evidence documents – but this way of work is still inconvenient because the developers must carefully read recommendations, check requirements and think about the necessary information to be provided in every new document each time they begin a project.

Although this guidelines-based approach helps the developers to work out documentation, it still does not allow to get rid of inefficient and time-consuming work, which is why some software aiding tools were applied to support the work with documents templates. Most of the software tools are dedicated only to preparing security specification documents (ST, PP) [Higaki 2010]. For example, the MS Windows application "CC Toolbox" sponsored by the National Information Assurance Partnership (NIAP, the US government initiative) was used to assist users in writing ST and PP but is no longer supported and available. In the paper [*GEST: A generator…* 2009] a generator of security target templates, named "GEST" was presented that can automatically generate security target templates from already evaluated and certified security targets. One of the Spanish CC licensed laboratories, "Applus", presented a tool that automates the writing of evidence documents [Kane 2008]. Another software tool, "TL SET", was introduced by Trusted Labs [Trusted-labs 2013]. It is a smart editor for Security Targets and Protection Profiles. It integrates predefined libraries of the Common Criteria functional and assurance requirements and a user-friendly graphical interface to fill out the documents. There are also tools with built-in OWL language (OWL – Web Ontology Language) [Białas 2009, 2011a; 2011b; 2012]. These tools are dedicated to building functional specification of the TOE and security problem definition.

So far all the solutions based on guidelines and computer tools have concerned mainly two basic documents, ST and PP. This paper presents a solution which allows to produce all the necessary documents and uses context-sensitive help based on the CC standard and supplementary documents. The next section describes the basics of the CC methodology which is to be supported by the computer tool.

3. The Common Criteria methodology

The CC methodology comprises three major processes.

1) IT security development – this process is based on security analyses and identifies a security problem which has to be countered by security functions of the TOE. At this stage a special document Security Target (ST) is worked out. In ST, to put it briefly, security functional requirements specification (SFRs) describes how security measures should work in the TOE to effectively counter the identified threats. The requirements are described in CC by functional components which are grouped in 11 classes referring to certain security issues as: security audit, communication, cryptographic support, user data protection, identification and authentication, security management, privacy, protection of the TSF (TOE security function), resource utilization, TOE access, trusted path/channels.

These security functions should be implemented at a given assurance level which is determined by security assurance requirements (SARs) grouped in a given EAL (Evaluation Assurance Level) package. The SARs set the range and details of the TOE development and the TOE evaluation processes. As a result of the IT security development process, the ST document is worked out which is the starting point for the next process.

2) TOE development – the aim of this process is to made the TOE (hardware, software) and to elaborate the evidence documents implied by the SAR components of the claimed EAL. The evidence documents can have different forms, starting from manuals, user guides, configuration managements plans, through to the results of independent examinations or observations carried out by the evaluators, ending with the security target or protection profile. The evidence documents should be prepared according to the following assurance classes: development (ADV), life-cycle support (ALC), tests (ATE), guides (AGD), vulnerability analysis (AVA). The results of this process is evaluation evidence for the given IT product which are used in the next security evaluation process.

3) IT security evaluation – this process is conducted by an independent certified laboratory according to the CEM methodology. A positive assessment of the product along with its documentation is confirmed by a certification body. The certificate confirms that the IT product is compliant with the declared EAL. The certificates are published on the Common Criteria portal [CC Portal 2013]. Evaluation Assurance Levels are interpreted as follows: EAL1 – means that the TOE was functionally tested, EAL2 – the TOE was structurally tested, EAL3 – the TOE project was methodically tested and checked, EAL4 – the TOE was methodically designed, tested and reviewed, EAL5 – the TOE was semi-formally designed and tested, EAL6 – the TOE project was semi-formally verified design and tested, EAL7 – the TOE project was formally verified design and tested.

Common Criteria does not define the product security features or functionality, but it provides an assurance that the process of specification, implementation and evaluation of the product has been made in a rigorous manner. EALs reflect the degree of confidence a user can have in the results of the evaluation and performance of the TOE. The lower assurance levels, EAL 1 through 4, concern most products and do not require an evaluation of the software, only of the development process and documentation. These lower levels are recognized under CCRA, whereas the higher EALs are generally country-specific [Jackson 2007] and require a source code of the product to be analyzed.

In the IT security evaluation process, evidence documents are verified according to the security assurance requirements which were the source of the design patterns. Due to the fact that a large number of evidence documents must be prepared, in the next subsection it is shown that there is a necessity to prepare the design patterns for all SARs.

3.1. Evidence documents

In the Common Criteria evaluation, the process security functions of the TOE are evaluated according to the security assurance requirements (SARs) in the given EAL.

The Security Target (ST) is the most important evidence document. The ST describes a specific TOE and is written by the developer. The ST can be based on a document called the Protection Profile (PP). The PP describes the general requirements for a TOE type and is used as a template for many different ST documents. The ST consists of a security problem definition, security objectives, security requirements, a summary specification – showing how the security functions are implemented in the TOE. The ST document claims conformance with the declared EAL and this determines all requirements which have to be fulfilled by the product and described in evidence documentation.

The EAL package consists of assurance components which are organized into classes and families. The following descriptions of classes also include their abbreviated names (in brackets) which are commonly used in the CC standard. The Protection Profile Evaluation (APE) and Security Target Evaluation (ASE) classes describe the content and presentation of the PP and ST documents. The Development (ADV) class encompasses six families and nineteen components, it provides information about the structuring of the TOE security functionality. The Guidance Documents (AGD) class is divided into two families (with one component for each family), it provides the requirements for preparative and operational user guides. The Life-cycle Support (ALC) class consists of seven families and twenty one components, it concerns the aspects of establishing discipline and control in the TOE development and maintenance during its whole life-cycle. The Tests (ATE) class encompasses four families and twelve components, it provides an assurance that the TOE security functions were tested and they operate according to their design descriptions. The Vulnerability Assessment (AVA) class has only one family with five components, it addresses the possibility of exploitable vulnerabilities introduced in the TOE or in its development or operational environment. The Composition (ACO) class encompasses five families and eleven components, it ensures that the TOE composed of other evaluated TOEs will operate securely. For instance, the EAL 4 package has eighteen components (including one optional), and for each one (names in brackets) a proper evidence document has to be prepared, as shown below:

- TOE security architecture description (ADV_ARC.1);
- TOE functional specification with interfaces of security functions (ADV_FSP.4);
- the implementation representation of security functions (ADV_IMP.1);
- TOE project specification with subsystems and modules (ADV_TDS.3);
- an operational user guidance (AGD_OPE.1);
- the preparative procedures of operational environment, TOE installation procedures, calibration (AGD_PRE.1);
- the capabilities of configuration management system (ALC_CMC.4);
- a scope of the configuration management system (ALC_CMS.4);
- procedures for delivery of the TOE to the consumer (ALC_DEL.1);
- physical, procedural, personnel, and other security measures that are necessary to protect the confidentiality and integrity of the TOE design and implementation in its development environment (ALC_DVS.1);
- a life-cycle model to be used in the development and maintenance of the TOE (ALC_LCD.1);
- tools and techniques are an aspect of selecting tools that are used to develop, analyze and implement the TOE (ALC_TAT.1);
- confirmation that all of the TOE security functions interfaces (TSFIs) have been tested (ATE_COV.2);
- testing of the security enforcing modules (ATE_DPT.2);
- functional testing, test plans, expected test results and actual test results (ATE_FUN.1);
- independent testing – verification of the developer testing and performing additional tests by the evaluator (ATE_IND.2);
- vulnerability analysis of the development environment and anticipated operation of the TOE (AVA_VAN.3);
- flaw remediation procedures describing the methods for dealing with all types of flaws encountered in the TOE (ALC_FLR.1, ALC_FLR.2) – optional at any EAL.

On the basis of all assurance components taken from every EAL package, the design patterns were worked out. The next subsection describes the main steps of the methodology thanks to which the computer-aided tool was worked out in the CCMODE project.

3.2. Applying the CC methodology

In the first part of the CCMODE project the design patterns for all security assurance requirements (SARs) were prepared. The patterns are in the form of MS Word documents with predefined chapters, sections and data fields. Next, the patterns were validated on the basis of several projects concerning a software system and intelligent sensors [Białas 2009, 2011a; 2011b; *Zastosowanie wzorców*… 2013; Broja et al. … 2011]. The developers used selected design patterns to make evidence documentation of their software and hardware IT products. As a result of the validation, necessary changes and amendments were incorporated into the patterns. In changing the patterns, the CCMODE project team members had to: specify more precisely the comments and tips describing data fields, specify more precisely the names of the data fields, remove the surplus (not used) data fields, update references, add new or update the chosen footnotes, alter or add new English terms, and improve some translation of Polish terms and definitions in order to make them consistent with the original English terms.

Furthermore, the developers made basic functional assumptions for the computer tool concerning: management of the project and development environment, configuration management according to the CC requirements, support for elaborating evidence documents, support for versioning of documents and products, support for tests and security flaws remediation, self-evaluation of evidence documents, an easy access to knowledge about the CC standard and related documents.

In the next project stages, on the basis of functional assumptions, a prototype system was developed. The prototype was validated during the development of some software- and hardware (with built-in firmware) products [*Komputerowe wspomaganie*... 2012]. The results of case studies helped to apply improvements in the tool concerning: project management, security analyses for the product, elaborating evidence documents, self-evaluation of documents, and incorporating the new definitions of components according to the CC requirements.

As a result, the CCMODE Tools system was worked out. The system integrates:

- project and development environment management module for the initialization of new projects and their configuration according to the declared EAL;
- configuration management module according to the CC requirements;
- documents generator (GenDoc) module to work out evidence documents based on the design patterns;
- the auditing module of the TOE development environment (based on surveys) and self-evaluation module of evidence documentation (based on CEM);
- integrated external systems for security analyses, versioning, bug tracking, testing.

Apart from the system, other products were developed in the CCMODE project. They include the design patterns, methodology of deployment and management of the CC development environment, and knowledge base.

The system can be integrated with other security standards, like an information security management standard (ISMS, based on ISO/IEC 27001) or business continuity management standard (BCMS, based on BS 25999) [Bagiński, Białas 2012].

Thanks to the applied development rigour, as well as independent evaluation, certified products are recognized as more reliable and dependable, but the usage of the CC methodology is still difficult and complex for developers who are not familiar enough with it. Additionally, the cost of IT products development and evaluation is high. This is why in the CCMODE project a lot of effort was put into working out the computer tool which could support the fulfillment of all three CC methodology processes. The following chapters describe the functionality of the software system which implements the design patterns.

4. Computer-aided tool

Developers use the software tool to start the project of an IT product in accordance with the chosen EAL level. They configure the necessary external systems and deliver basic information about the type of the product, life-cycle model of the TOE, roles and duties of the system users, software and hardware tools used during the TOE development, security standards and regulations used in the development environment.

The actions mentioned above were next implemented in dedicated modules of the CCMODE Tools system. The following subsections describe the general model and main modules of the system.

4.1. General model of CCMODE Tools

A general model of the system is depicted in Figure 1. The model consists of the Environment Management Tool (EMT), documents generator (GenDoc), knowledge base, evaluation module, external supporting systems, optional security systems (BCMS or ISMS) which can be used as an additional source of assurance to the whole development environment [*Komputerowe wspomaganie*... 2012].

EMT is the main module which supports the configuration and management of the IT projects. The module allows:

- management of the users and their roles in the system and project;
- configuration of the project, which includes: type of project, declared EAL, a life-cycle model, tools and techniques used in the TOE development, subcontractors, procedures, standards, regulations, etc.;
- configuration of the system, which includes: integration of external supporting systems, the system documentation, external services, review of system logs;
- review of projects and their data sources.

The knowledge base is a source of context-sensitive help about the CC requirements and guidelines. It includes the electronic version of the Common

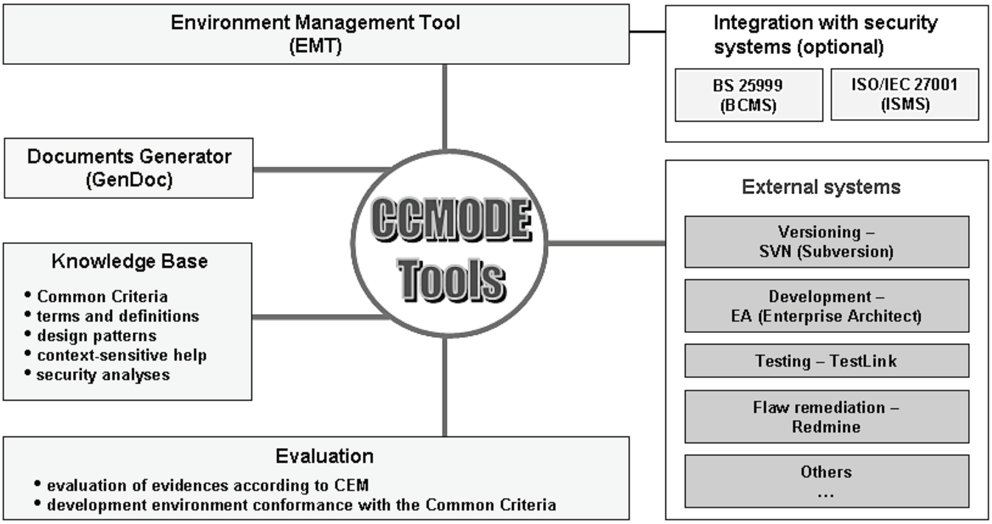

Environment Management Tool (EMT)
Integration with security systems (optional)
BS 25999 (BCMS)
ISO/IEC 27001 (ISMS)
Documents Generator (GenDoc)
CCMODE Tools
External systems
Versioning – SVN (Subversion)
Development – EA (Enterprise Architect)
Testing – TestLink
Flaw remediation – Redmine
Others …
Knowledge Base
• Common Criteria
• terms and definitions
• design patterns
• context-sensitive help
• security analyses
Evaluation
• evaluation of evidences according to CEM
• development environment conformance with the Common Criteria

Figure 1. The general model of the CCMODE Tools system

Source: own elaboration based on [Rogowski 2013].

Criteria standard, easily accessible by any Web browser and by any module of the CCMODE Tools system. It includes design patterns, terms and definitions, and the guidelines that help to resolve typical security problems with the use of predefined security objectives, threats, assumptions, and security policies. The main goal of the knowledge base is to help and assist the developers at any stage of the TOE development and evidence documents' preparation.

The evaluation module is divided into two parts. The first concerns the auditing module for verification of the development environment conformance with the CC requirements. The second concerns the evaluation of evidence documents according to the CEM methodology.

There are also external systems in CCMODE Tools which support:

- versioning of projects artifacts – Subversion (SVN) application;
- modeling, development and security analyses which are made with the use of UML (Unified Modeling Language) – Enterprise Architect (EA);
- flaws reporting and flaws remediation – Redmine;
- management and planning of TOE tests – TestLink.

After project configuration the developer can start writing evidence documents by using the documents generator GenDoc.

4.2. Design patterns within documents generator

This section shows, using the example of an ST document, how the design patterns are implemented in the computer tool. The documents generator (GenDoc) is used for editing evidence documents based on the design patterns. In order to evaluate the TOE, an ST document and accompanying documents must be prepared. These additional documents are determined by the chosen EAL and its SAR components. The precise details of the security development procedure and working out the evidence documents in the context of biometric devices can be found in [Białas 2013].

The precise details, structure and data fields of the pattern were elaborated on the basis of components and elements of SARs. For instance the ST pattern was elaborated on the basis of the ASE (ST evaluation) class. The ASE class describes the obligatory content of the document, which is presented in Figure 2 in the form of chapters and subsections. The chapters must be filled in according to the SAR requirements and to the CEM methodology which is used for evidence evaluation.

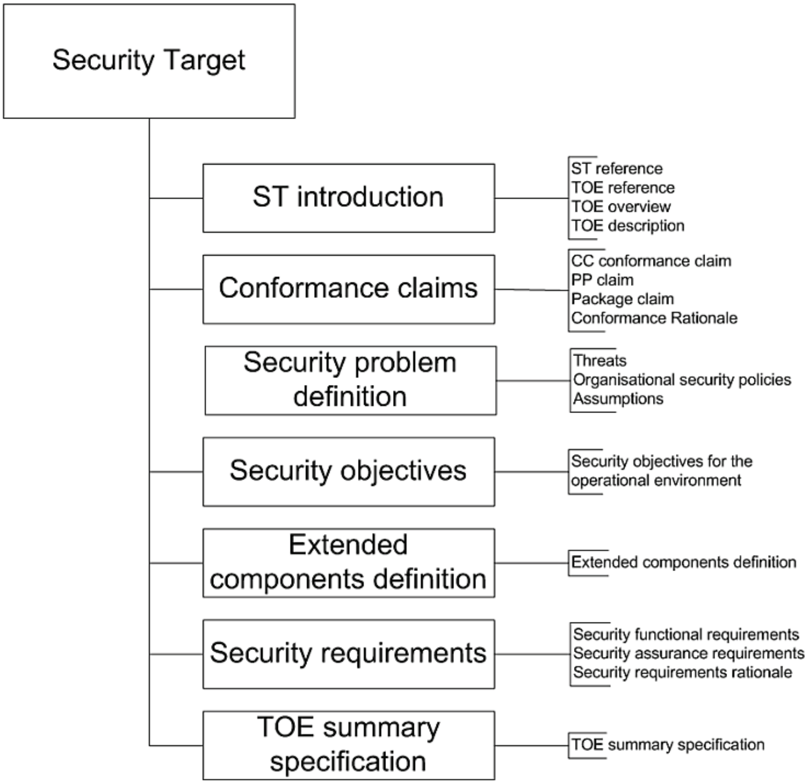
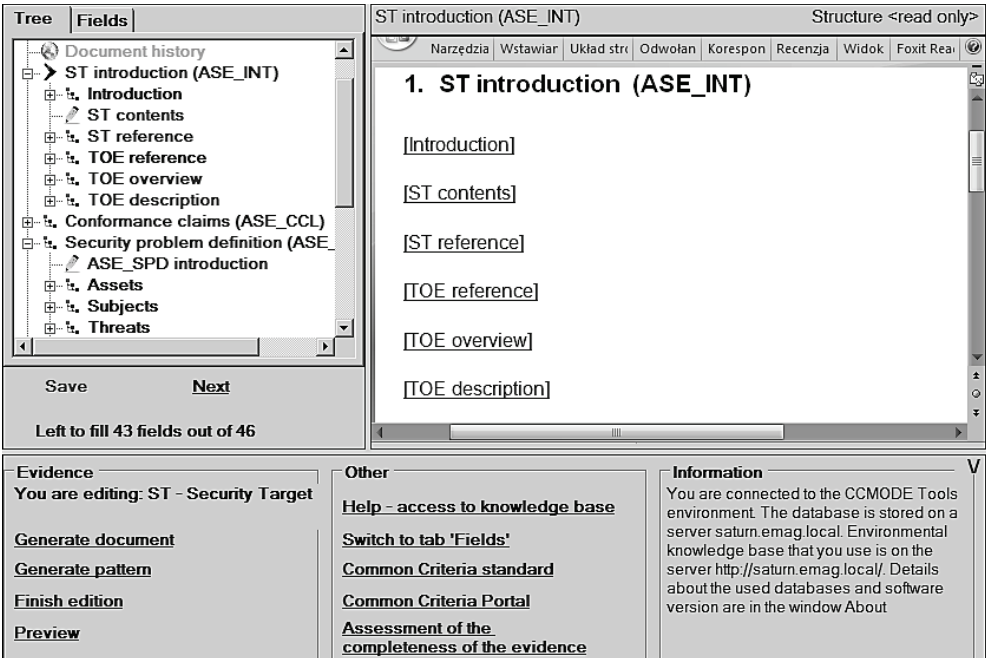

Security Target
ST introduction
ST reference
TOE reference
TOE overview
TOE description
Conformance claims
CC conformance claim
PP claim
Package claim
Conformance Rationale
Security problem definition
Threats
Organisational security policies
Assumptions
Security objectives
Security objectives for the operational environment
Extended components definition
Extended components definition
Security requirements
Security functional requirements
Security assurance requirements
Security requirements rationale
TOE summary specification
TOE summary specification

Figure 2. The structure of the ST design pattern

Source: [*CC Part 1*… 2012.]

The design pattern includes special data fields and footnotes with hints and tips, based on SARs and CEM, which help the developers in preparing the document. In the same way the rest of the design patterns were worked out according to every SAR component.

The structure of the "paper" version of the patterns, along with context-sensitive help and data fields, was the starting point for the software implementation of the patterns.



You are connected to the CCMODE Tools environment. The database is stored on a server saturn.emag.local. Environmental knowledge base that you use is on the server http://saturn.emag.local/. Details about the used databases and software version are in the window About

Figure 3. The GenDoc window with the implemented ST design pattern

Source: own elaboration based on [Rogowski 2013].

Every pattern in GenDoc was prepared as a tree of data fields which represent chapters, sections and subsections of the output document. The tree is based on the requirements of the given SAR component. The colors of branches show which fields have to be filled in by the user (red ones), which are already filled (black ones), and which are without any data (brown ones). The gray colored fields are automatically filled in with the information taken from the knowledge base and external modules: EA, EMT, SVN, TestLink.

Figure 3 depicts the ST design pattern already implemented in the GenDoc module. In order to complete the document, the user must follow all the tree branches and find out which fields have to be completed. Every field has its own context-sensitive help which gives the necessary guidelines and hints about the information to be delivered.

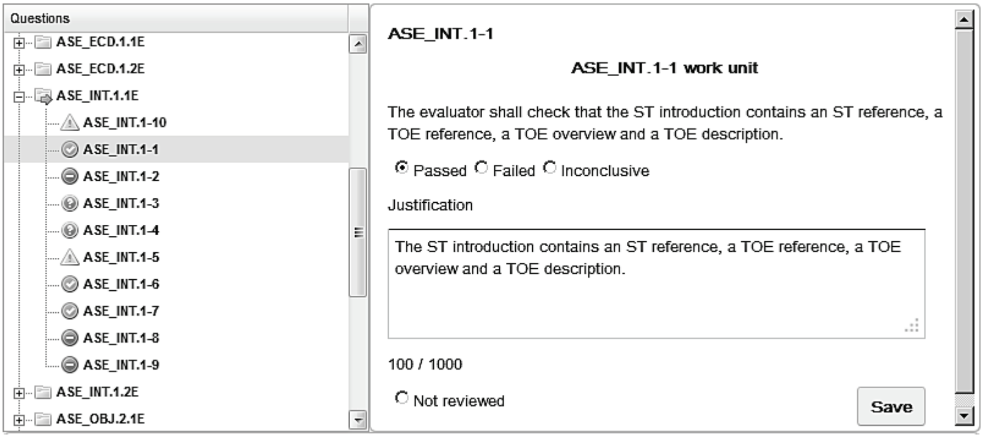
4.3. Context-sensitive help

The preparation of data fields content can be facilitated by context-sensitive help. This help is accessible from the main window of GenDoc by the link “Help – access to knowledge base”. There were five types of help applied: “ready to use” – comprises a text which is ready to use by the user without the necessity to change any information in it; “Common Criteria help” – comprises all the information about the standard; “hints” – these are interpretations, tips and guidelines; “example” – is an optional text which illustrates what kind of data can be written in the given field; “data source” – indicates an external system which is the source of data for the given data field. All the design patterns implemented into the CCMODE Tools system have similar representations. They contain data fields with precise instructions on how to generate a complete evidence document.

At every stage of the edition process the data fields can be reviewed and checked. Verification of the document can be done with the use of the evaluation module as described in the next section.

4.4. Self-evaluation of evidence documents

After completing all the information in the pattern, the user can verify the output document by using an evaluation module which is a part of the EMT system (Figure 4). This module enables to check the document according to the CEM evaluation methodology.



ASE_INT.1-1

ASE_INT.1-1 work unit

The evaluator shall check that the ST introduction contains an ST reference, a TOE reference, a TOE overview and a TOE description.

● Passed ○ Failed ○ Inconclusive

Justification

The ST introduction contains an ST reference, a TOE reference, a TOE overview and a TOE description.

100 / 1000

○ Not reviewed

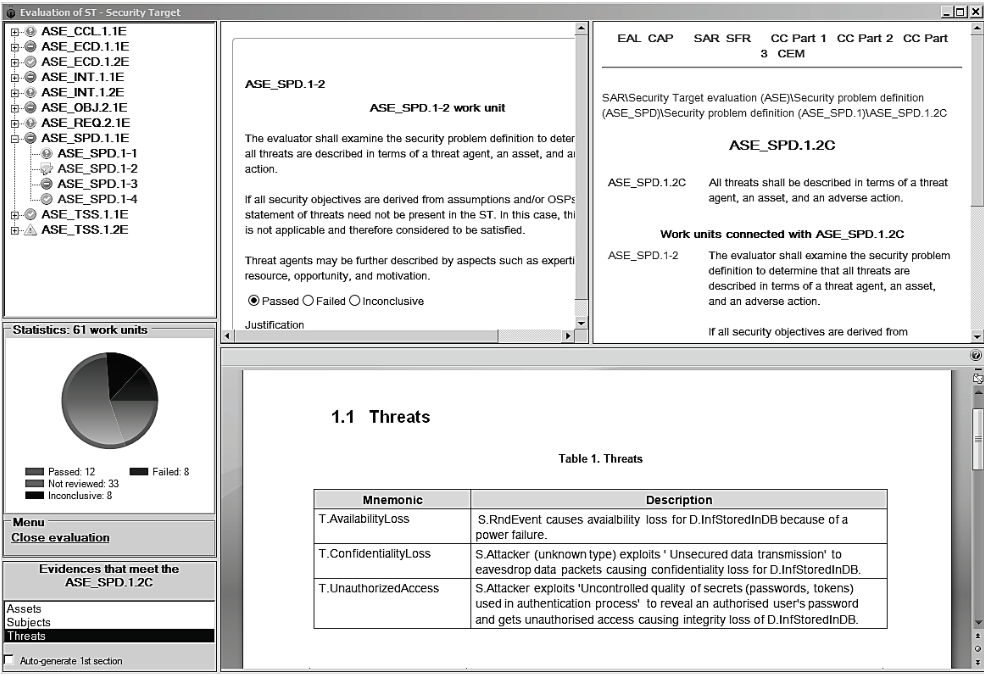
Figure 4. The evaluation module of the EMT system

Source: own elaboration based on [Rogowski 2013].

In general, the methodology specifies elements which describe the evaluation tasks to be done by the evaluator. These tasks give precise information on how each security assurance component should be checked. Every task consists of a set of questions referring to the content and form of the evidence document. These questions are grouped in the so called work units. The answers lead to work units verdicts which can have one of three possible states: pass, fail or inconclusive. Each verdict needs a brief justification. All verdicts are initially inconclusive and remain so until either a pass or fail verdict is assigned. Verification of the evidence document is positive when all the verdicts have been passed.

The evaluation module consists of work units with their detailed descriptions and has an answer form with a built-in justification field as depicted in Figure 4. The developer has to answer all these questions which pertain to the verified document.

The enhanced version of the evaluation module was applied in GenDoc where the work units are directly connected to the relevant chapters and subsections of the evidence document in order to make the verification process easier and faster. In this way the developer can see the current content of the evidence chapter, the relevant work unit, and a description of the given SAR component in one GenDoc window, as depicted in Figure 5.



ASE_SPD.1-2

ASE_SPD.1-2 work unit

The evaluator shall examine the security problem definition to deter all threats are described in terms of a threat agent, an asset, and a action.

If all security objectives are derived from assumptions and/or OSPs statement of threats need not be present in the ST. In this case, thi is not applicable and therefore considered to be satisfied.

Threat agents may be further described by aspects such as experti resource, opportunity, and motivation.

● Passed ○ Failed ○ Inconclusive

Justification

SAR\Security Target evaluation (ASE)\Security problem definition (ASE_SPD)\Security problem definition (ASE_SPD.1)\ASE_SPD.1.2C

ASE_SPD.1.2C

ASE_SPD.1.2C All threats shall be described in terms of a threat agent, an asset, and an adverse action.

Work units connected with ASE_SPD.1.2C

ASE_SPD.1-2 The evaluator shall examine the security problem definition to determine that all threats are described in terms of a threat agent, an asset, and an adverse action.

If all security objectives are derived from

1.1 Threats

Table 1. Threats

Mnemonic	Description
T.AvailabilityLoss	S.RndEvent causes avaialbility loss for D.InfStoredInDB because of a power failure.
T.ConfidentialityLoss	S.Attacker (unknown type) exploits ' Unsecured data transmission' to eavesdrop data packets causing confidentiality loss for D.InfStoredInDB.
T.UnauthorizedAccess	S.Attacker exploits 'Uncontrolled quality of secrets (passwords, tokens) used in authentication process' to reveal an authorised user's password and gets unauthorised access causing integrity loss of D.InfStoredInDB.

Figure 5. The evaluation module in GenDoc

Source: own elaboration.

After verification, the complete document can be generated as an MS Word document and saved in the SVN repository. This document can be edited in a standard MS Word editor. The document has a fixed structure with chapters, sections and subsections. It also contains footnotes with hints and guidelines.

5. Conclusions

This paper presented the computer-aided tool which supports the development of IT security enhanced products according to the Common Criteria standard. The standard allows to develop IT products with built-in security functions with the claimed assurance level. This assurance is acquired thanks to rigorous development processes and independent evaluation and certification processes. However, using the Common Criteria standard and preparing for the evaluation processes is a very difficult and complex task for the developers. Without design patterns and supporting tools, applying the CC requirements in IT projects is costly and time consuming. This is why the CCMODE Tools system was developed in order to support the TOE development, security analyses, and elaborating evidence documentation. Now the developers do not have to prepare evidence documents from the very beginning. They can concentrate only on writing the proper content which is now managed and controlled by the modules of the system. The proposed solution, based on the patterns-based approach, improves the CC development processes. It overcomes the lack of knowledge and experience of the developers.

This paper also described the design patterns of evidence documents. The patterns were positively checked and validated by the developers who asked for some automation functions. These functions were next implemented into the computer-aided tool. The software tool facilitates and speeds up the development process and improves the quality of evidence, which becomes more consistent and includes all details required by the CC assurance requirements.

The CCMODE Tools system gives a great chance to prepare all documentation for a successful Common Criteria evaluation because additional self-evaluation and verification functions were also applied in the tool. They offer a practical way of document verification before the main CC evaluation process conducted by a certified laboratory.

Future work will be focused on building a standalone, independent GenDoc and EA applications which could work without the EMT framework. This is awaited by some developers who want to focus only on basic security analyses of the TOE along with its evidence documentation.

References

Bagiński J., Białas A., *Validation of the software supporting information security and business continuity management processes*, [in:] *Complex Systems and Dependability*, AISC, vol. 170, eds. W. Zamojski, J. Mazurkiewicz, J. Sugier, T. Walkowiak, J. Kacprzyk, , Springer-Verlag, Berlin Heidelberg 2012, pp. 1-18.

Białas A., *Common Criteria related security design patterns for intelligent sensors – knowledge engineering-based implementation*, "SENSORS", vol. 11, issue 8, DOI: 10.3390/s110808085, 2011a, pp. 8085-8114.

Białas A., *How to develop a biometric system with claimed assurance*, IEEE Xplore Digital Library, in press, 2013.

Białas A., *Patterns improving the Common Criteria compliant IT security development process,* [in:] *Dependable Computer Systems*, AISC, vol. 97, eds. W. Zamojski, J. Kacprzyk, J. Mazurkiewicz, J. Sugier, T. Walkowiak, Springer-Verlag, Berlin Heidelberg 2011, pp. 1-16.

Białas A., *Security-related design patterns for intelligent sensors requiring measurable assurance*, "Electrical Review" 2009, vol. 85 (R. 85), no. 7/2009, ISSN 0033-2097, pp. 92-99.

Białas A., *Semiformal Common Criteria compliant IT security development framework, "*Studia Informatica" 2008, 29, no. 2B(77).

Białas A., *Specification means definition for the Common Criteria compliant development process – an ontological approach*, [in:] *Complex Systems and Dependability*, AISC, vol. 170, eds. W. Zamojski, J. Kacprzyk, J. Mazurkiewicz, J. Sugier, T. Walkowiak, ISBN 978-3-642-30662-4, Springer--Verlag, Berlin Heidelberg 2012, pp. 37-54.

Broja A., Cała D., Małachowski M., Śpiechowicz K., Szczurek A., *Zastosowanie metodyki Common Criteria podczas procesu projektowania urządzeń na przykładzie czujnika gazometrycznego*, Instytut Technik Innowacyjnych EMAG, MIAG 5 (483), Katowice 2011, pp. 12-18.

CC Part 1, *Common Criteria for Information Technology Security Evaluation (Version 3.1, Revision 4) Part 1: Introduction and general model (ISO/IEC 15408-1)*, CCMB, September 2012.

CC Part 2, *Common Criteria for Information Technology Security Evaluation (Version 3.1, Revision 4) Part 2: Part 2: Security functional requirements (ISO/IEC 15408-2)*, CCMB, September 2012.

CC Part 3, *Common Criteria for Information Technology Security Evaluation (Version 3.1, Revision 4) Part 3: Part 3: Security assurance requirements (ISO/IEC 15408-3)*, CCMB, September 2012.

CC Portal, http://www.commoncriteriaportal.org/ [accessed July 2013].

Certification Report – BSI-DSZ-CC-0694-2012, SmartApp SIGN 2.2 from Polska Wytwórnia Papierów Wartościowych S.A., BSI (ger. Bundesamt für Sicherheit in der Informationstechnik), Bonn, 6 February 2012.

Common Methodology for Information Technology Security Evaluation (Version 3.1, Revision 4) Evaluation Methodology, CCMB, September 2012.

Guidelines for developer documentation according to Common Criteria Version 3.1, BSI (ger. Bundesamt für Sicherheit in der Informationstechnik), 2007.

Guidelines for evaluation reports according to Common Criteria Version 3.1, Version 2.00 for CCv3.1 rev. 3, BSI (ger. Bundesamt für Sicherheit in der Informationstechnik), 2010.

Higaki W.H., *Successful Common Criteria evaluations. A practical guide for vendors*, Create Space Independent Publishing Platform, 2010.

Horie D., Yajima K., Azimah N., Goto Y., Cheng J., *GEST: A generator of ISO/IEC15408 Security Target templates*, [in:] *Computer and Information Science,* eds. R. Lee., G. Hu, H. Miao, SCI 208, Springer-Verlag, Berlin Heidelberg 2009, pp 149-158.

International Common Criteria Conference (13th), http://www.iccc2012paris.com/en/, Paris 2012 [accessed: July 2013].

ISO/IEC TR 15446 – Information technology – security techniques – guide for the production of Protection Profiles and Security Targets, JTC 1/SC27, Berlin 2009.

ITSEC – Information Technology Security Evaluation Criteria (ITSEC): Preliminary Harmonized Criteria. Document COM(90) 314, Version 1.2, Commission of the European Communities, June 1991.

Jackson W., *Under attack*, GCN, http://gcn.com/articles/2007/08/10/under-attack.aspx, August 10, 2007.

Kane I., *Automated tools for supporting CC design evidence*, [in:] *9th International Common Criteria Conference*, Jeju 2008.

Komputerowe wspomaganie procesu rozwoju produktów informatycznych o podwyższonych wymaganiach bezpieczeństwa, ed. A. Białas, ISBN 978-83-932737-8-2, Wydawnictwo Instytutu Technik Innowacyjnych EMAG, Katowice 2012.

Rogowski D., *Software Implementation of Common Criteria Related Design Patterns*, IEEE Xplore Digital Library (to be published), 2013.

Rogowski D., Nowak P., *Pattern based support for Site Certification* [in:] *Complex Systems and Dependability*, AISC, vol. 170, pp. 179-193, eds. W. Zamojski, et. al., Springer-Verlag, Berlin Heidelberg 2012.

The PP/ST guide, *Version 1, Revision 6.2*, BSI (ger. Bundesamt für Sicherheit in der Informationstechnik), August 2007.

Trusted-labs, *www.trusted-labs.com*, [accessed: May 2013].

Zastosowanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria, ed. A. Białas, ISBN 978-83-932737-2-0, Wydawnictwo Instytutu Technik Innowacyjnych EMAG, Katowice 2011.

KOMPUTEROWE NARZĘDZIE WSPOMAGAJĄCE OPARTE NA WZORCACH PROJEKTOWYCH ZGODNYCH ZE WSPÓLNYMI KRYTERIAMI

Streszczenie: Artykuł opisuje wyniki projektu badawczo-rozwojowego, którego celem było opracowanie komputerowego narzędzia do wspomagania rozwoju produktów informatycznych z wbudowanymi zabezpieczeniami. Narzędzie gwarantuje, że wszystkie środki zabezpieczające są implementowane w produkcie zgodnie z wymaganiami standardu ISO/IEC 15408 „Wspólne Kryteria do oceny zabezpieczeń informatycznych" (*Common Criteria for Information Technology Security Evaluation*). Aktualnie funkcjonuje kilka ograniczonych rozwiązań, które wspomagają projektantów w używaniu metodyki *Common Criteria*. Zaproponowane narzędzie wspomaga trzy podstawowe procesy: projektowania zabezpieczeń, projektowania produktu oraz oceny produktu, jak również wspomaga opracowanie specjalnej dokumentacji dowodowej bazującej na wzorcach projektowych. Projektanci użyli komputerowego narzędzia w trakcie projektowania oprogramowania i rozwiązań sprzętowych, wykazali też, że narzędzie ułatwia i przyspiesza realizację procesów rozwojowych produktów informatycznych o podwyższonych wymaganiach bezpieczeństwa.

Słowa kluczowe: wspólne kryteria, uzasadnione zaufanie do zabezpieczeń, wzorce projektowe, komputerowe narzędzie wspomagające.