Software Support for Common Criteria Security Development Process on the Example of a Data Diode

Dariusz Rogowski

Institute of Innovative Technologies EMAG, 40-189 Katowice, Leopolda 31, Poland
drogowski@emag.pl

Abstract. The data diodes are very often used to protect users’ networks and sensitive data and that is why additional assurance of those devices is demanded. This assurance can be obtained by applying the Common Criteria security development process. The process is very difficult and time-consuming specially for those not familiar with the standard. Although there are many guidelines and templates telling how to define the security problem still there is a lack of computer aiding tools. This paper describes the plug-in application which supports identification of protected assets, threats, security objectives and security functions – the main elements of security specification. The tool facilitates and speeds up the security development process of IT products.

Keywords: Common Criteria, security development, a data diode.

1 Introduction

Security of networked systems has received much attention in recent years due to many cyber attacks and leaks of sensitive information. There are devices and systems on the market which can help to protect higher security classified networks. For instance, it could be both software and hardware solutions such as firewalls or smart switches. Among them there is one very interesting and simple-structured hardware device that can prevent data leakage of confidential or classified data. This is the so called data diode which makes one-way link between a high security classified network and a low security classified network [1-5].

The data diode is built of fiber optic transceivers which enable one way data transmission. Fiber optic technology is used to minimize the electromagnetic radiation of a device by which transmitted data could be eavesdropped. The data diode connection ensures that unwanted access to the protected network is not possible while there is still free access to data sources placed outside. For instance, in the protected zone, anti-virus applications, operating systems, emails can be updated freely by downloading necessary data from public networks (e.g. the Internet) but at the same time no information can be extracted from the protected network. These devices are often used in the defense and infrastructure environments where security is critical. Many of them are compliant with rigorous Critical Infrastructure Protection (CIP) standards or regulations established by such organizations as NRC (U.S. Nuclear Regulatory
Commission), NIST (National Institute of Standards and Technology) or NIAP (National Information Assurance Partnership).

The data diode, like other IT devices, can be additionally checked and evaluated by an independent body according to a stringent security standard – Common Criteria (CC) also known as ISO/IEC 15408 [6-8]. In the result of evaluation a certificate can be issued stating that the target of evaluation (TOE, i.e. a device) fulfilled all requirements congruent with the given Evaluation Assurance Level (EAL). This level tells a user how reliable the security measures built in the evaluated product are. On the EAL basis the user can decide whether to accept the risk of exposing the product to threats or not. According to the standard there are seven levels ranging from EAL1 to EAL7. Most of the certified IT products have middle-ranged levels (EAL3 – EAL4) due to the rising costs of evaluation and development processes at higher levels [9]. However, data diodes have very often higher EALs (EAL4+ or EAL7+) because of their relatively simple hardware structure that does not significantly increase the costs of the evaluation process [10], [11].

The developers have to prepare not only a product itself for the evaluation process but also some special accompanying evidence documents. These documents are key factors of successful evaluation results. That is why preparing them in a proper manner is a big challenge for developers not familiar with the rules of the Common Criteria. So far relatively little attention has been paid by researchers to support and make this task easier. Later in this paper it will be demonstrated how to help developers in preparing a part of a Security Target (ST) document by using a software tool made by the Institute EMAG in one of R&D projects [12].

The Security Target is the most important document which, in general, specifies “what is to be evaluated”. ST is a security specification on a relatively high level of abstraction which describes how security measures should work and how reliable they are. These measures are presented by SFRs (Security Functional Requirements) and SARs (Security Assurance Requirements) components which are a kind of semiformal language of the Common Criteria standard. Thanks to the CC components all documents can be built in the same way by different developers for different types of products. The documents can be also verified according to one Common Evaluation Methodology (CEM) [13].

The CEM methodology defines evaluation activities and work units to be done by evaluators in order to issue verdicts about security measures implemented in a product and described in evidence documents. As a result, the evaluators can assess the documents in a relatively easy way because they have the ready-to-use evaluation methodology. But what about the developers? In contrast to the evaluators, they have not got too many options for help. Even the standard itself, very extensive, with lots of details and hundreds of components, is very difficult to use by inexperienced users. Of course there are many consulting companies on the market but their services are very expensive. Some possibilities of additional costs mitigation were proposed and described in the previous papers [14], [15]. The design patterns of evidence documents and computer tools were presented there as the way to support developers in elaborating necessary TOE documentation.
The literature review and state of the art showed that there were very few solutions which could help developers to fulfill all the requirements of the standard. Until now achieving the CC requirements has been still a very difficult and time-consuming task. There were also many guidelines, supporting documents with hints and tips and even templates of ST and other evidence documents [16-20]. Although such an approach improves developers’ work, it results in an unacceptable number of analyses of hundreds of the CC components that have to be done by the developers on their own. That is why using only guidelines is still inconvenient as such. The situation has not changed too much for better. There were only a few software tools supporting elaboration of the CC documents as it was also mentioned in [21], [22]. That is why a few years ago the CCMODE (Common Criteria compliant, Modular, Open IT security Development Environment) R&D project was launched by the Institute of Innovative Technologies EMAG [23] to improve the developers’ position.

The results of the project are methodology and software tools for developing and managing development environments of IT security-enhanced products for the purposes of their future evaluation and certification according to CC requirements. The software tool – called CCMODE Tools – integrates design patterns with documents generator application, knowledge base, evaluation methodology, and external supporting software dedicated for testing, flaws management and security analyses. The whole system can be used for a wide range of IT software and hardware devices or systems. The tool, along with the design patterns, was validated in a few projects concerning intelligent sensors [24], motion sensors [25], intelligent gas sensors for coal mines [26], and biometric systems [27]. The main features of the tool were presented in paper [28] whose main conclusion was that the design patterns supported by the software tool really facilitate and speed up development process and improve the quality of evidence documents.

Poland has not signed the Common Criteria Recognition Arrangement yet which allows to mutually recognize the CC certificates between the member states of this agreement. This is why the application of the CC standard is not obligatory in Poland. Yet there are some producers of special IT products (including data diodes) for military purposes who want their devices to be additionally accredited according to the CC requirements. One of the Polish producers of data diodes has started cooperation with the EMAG Institute in order to prepare a data diode to the CC accreditation process. As a result, an excellent opportunity emerged to make validation of the CCMODE Tools and to elaborate the trial version of the CC evidence documents of the product for the accreditation process at the same time. This example of cooperation shows that there could be a need for the future applications of the CC standard in Poland. The accreditation can be conducted by such Polish institutions as the Ministry of National Defense, the Internal Security Agency or Military Counterintelligence Service.

The purpose of this paper is to describe and examine a special plug-in application (another module of the CCMODE Tools system) dedicated to support security analyses of a product. This plug-in helps developers in elaborating the main parts of the ST document: a security problem definition (SPD) section which describes threats to product assets; a security objectives section which consists of statements resolving the
given security problem; a security requirements section which is presented in the semiformal language of SFRs and SARs components; a product summary specification containing security functions which should be implemented into the device in order to fulfill all security functional requirements. On the example of the data diode it will be demonstrated, in the results section of this paper, that the plug-in is an efficient and easy to use graphical tool for analyzing the security needs of the device and for elaborating the chosen sections of the ST document.

The paper is organized as follows. Section 1 presents the background of the Common Criteria standard and state of the art, and the main features of the data diode device. Section 2 describes three basic processes of the CC methodology and the general structure and features of the plug-in application. Section 3 delivers the results of the plug-in validation on the example of the data diode and presents main objects used to elaborate the chosen units of the ST document. Section 4 contains the results discussion and conclusions and states possible future work.

2 Methodology and Tools

The first possible way to create a new ST document is using a Protection Profile (PP) for the given type of products. If there is no suitable PP then a developer can use a few guidelines and templates issued by German Federal Office of Information Security (BSI) – the informal leader of researches in the field of the CC standard. This help documentation gives some advice on the structure and contents of evidence documents but developers have still many editorial activities left on their side.

The next two subsections of the paper describe respectively basic processes of the CC standard and the development stages of the plug-in software tool.

2.1 The Common Criteria Methodology for a Data Diode

Data diodes are products which can gain additional security assurance by applying the CC methodology. The positive evaluation results and certificate can be achieved by carrying out three basic processes: IT security development, TOE development, and IT security evaluation. These processes and the ST structure were described in detail in previous papers, e.g. [27], [28]. In the current paper, which concerns the range of the plug-in software support, only the most important activities of the security development process and the chosen sections of ST will be referred to and described. In the following paragraphs there were used some parts of the ST document for the CC certified data diode according to EAL4+ (called for short FFHDD – Fort Fox Hardware Data Diode) [10].

The IT security development process is based on security analyses whose purpose is to identify a product security problem and to resolve it by security objectives. That solution is described in the Security Target document in terms of security functional requirements (SFRs) which describe how security measures of the TOE should work to effectively counter the identified threats. In order to facilitate choosing the most suitable functional requirements for the given security objectives, the SFR
components are divided into 11 classes referring to such security issues as: security audit, communication, cryptographic support, user data protection, identification and authentication, security management, privacy, protection of the TSFs (TOE security functions), resource utilization, TOE access, trusted path/channels. These functional security requirements are next implemented into the device in the form of security functions during the TOE development process. These functions are also developed according to the security assurance requirements (SARs) of the claimed EAL.

As a result of the IT security development process the ST document is worked out. The complete document consists of the following sections: an ST introduction, a conformance claim, security problem definition (SPD), security objectives, extended component definition (optional), security requirements (SFRs and SARs), TOE summary specification. The plug-in software tool supports developers in elaborating all sections of the ST apart from the first ones: introduction and conformance claim which can be written in a standard text application. At the beginning of the IT security development process the security problem should be defined.

The SPD section defines the security problem that is to be addressed. It should be noted that usefulness of the ST document strongly depends on the quality of SPD and this is why it is worth to spend more time and resources to derive this section in a careful and reliable manner. What is more, the deriving process of SPD is outside the scope of the CC standard so developers can only follow the examples of the previously certified products to check how to make properly this section of the ST document. Here the plug-in software tool offers the developers very useful wizards and inferring mechanisms which make this process easier and quicker. The typical SPD consists of the following units: assets, threats, organizational security policies (OSP), and assumptions.

The security problem is understood as the danger of assets loss. So it is important to precisely identify all assets that have to be protected by the TOE and to identify all entities which interact with the TOE. For the above mentioned example of the certified data diode – FFHDD the protected asset is the sensitive information on the High Security Level network. The entities which can use this information can be authorized or not, and can be users or processes e.g.: an administrator, a user, a hacker, an update service. The threat unit describes the threats that are to be countered by the TOE, its operational environment, or combination of the two. A threat definition consists of an adverse action performed by a threat agent on an asset. In the example of the FFHDD device the threat T.TRANSFER was defined as “A user or process on the High Security Level network that accidentally or deliberately breaches the confidentiality of some High Security Level information by transmitting data through the TOE to the Low Security Level network”. The next unit of ST shows OSPs which are security rules, procedures, or guidelines imposed by an organization to the TOE or to the operational environment of the TOE. No OSPs were defined for the FFHDD product but an example of OSP can be a statement “Only users with system administrator privilege shall be allowed to set up and manage the data diode connection system”. The last unit of ST shows assumptions that are made on the operational environment in order to make it secure enough for the TOE. In such an environment the TOE is able to provide all its security functionalities without disruptions. Assumptions can be
made on physical, personnel and connectivity aspects of the operational environment. In the case of FFHDD the following assumptions were defined: A.PHYSICAL “The intended operation environment shall store and operate the TOE in accordance with the requirements of the High Security Level side”; A.NETWORK “The TOE is the only method of interconnecting the Low Security Level network and High Security Level network. This prevents a threat agent from circumventing the security being provided by the TOE through an untrustworthy product”. Once the complete SPD is defined the security objectives section of ST can next be elaborated.

The security objectives are the concise statements of the intended solution to the given problem defined by SPD. The security problem can be solved by two sets of objectives for the TOE and for the operational environment of the TOE. The first set shows what the TOE should do in order to protect the assets, e.g. for FFHDD: O.CONFIDENTIALITY “The information on the High Security Level side destination is kept confidential from the Low Security Level source”. The second set shows the goals that the operational environment should achieve, e.g. for FFHDD: OE.PHYSICAL “The intended operation environment shall be capable of storing and operating the TOE in accordance with the requirements of the High Security Level side”; OE.NETWORK “The TOE is the only method of interconnecting the Low Security Level network and High Security Level network”. In the end a developer should provide a rationale that security objectives counter all threats, enforce OSPs and upheld all assumptions. The next step is to translate the security objectives into the CC language of SFRs components.

The security requirements unit of ST consists of two groups of requirements: the security functional requirements (SFRs) – a translation of the security objectives for the TOE into a standardized, semiformal CC language; the security assurance requirements (SARs) – a description of how assurance is to be gained that the TOE meets the SFRs. The first group is made up from functional components taken from Part 2 of the CC standard and the second group are assurance components taken from Part 3 of the CC standard according to the claimed EAL (here EAL4+ for FFHDD). The SARs determine the range and details of the TOE development and security evaluation processes which are not in the focus of this paper. The SFRs are next implemented in the TOE security functions. In the example of FFHDD two functional components were selected which fulfill the TOE security objective for confidentiality: FDP_IFC.2 Complete Information Flow Control (FDP class – user data protection, IFC family – information flow control policy); FDP_IFF.1 Simple Security Attributes (IFF family – information flow control functions). Generally speaking these components permit the TOE security function to transmit sensitive information only from input (Low Security Level network) to output (High Security Level network) and not vice versa. The choice of proper SFRs is very difficult and depends on the developer’s experience and knowledge of the CC standard. Therefore there could be a vast potential demand for supporting this part of ST elaboration. The security requirements elaboration is finalized by their rationale. Next these requirements should be implemented in the TOE security functions which are described in the last section of ST – TOE summary specification (TSS).
The TSS section provides potential consumers of the TOE with a general technical description of how the product satisfies all the SFRs. In many cases the SFRs are gathered within one security issue, e.g. for FFHDD it is the user data protection class (FDP) described in the Part 2 of the CC standard. In the ST of this data diode is indicated that confidentiality of information is provided by using two functional requirements responsible for information flow control.

The IT security development process provides a set of security functions, which should be implemented into the TOE at the assurance of claimed EAL. The process of deriving security functions can be facilitated by the use of the plug-in software tool which was elaborated in the CCMODE R&D project.

2.2 Building the Plug-in Module

One of the CCMODE project results is the CCMODE Tools system. The system integrates: modules of the development environment management, design patterns, knowledge base, evaluation methodology, and external supporting software. Among the external applications there is the Enterprise Architect (EA) of the Sparx platform which was used as a basis for modeling, development and security analyses made in UML (Unified Modeling Language). In the CCMODE project a special plug-in for EA was worked out. The plug-in uses basic features of EA system and UML in order to support users in defining the TOE security problem and next in solving that problem by selecting security objectives and functional security requirements (SFRs).

At the beginning of the CCMODE project the survey of UML software development environments was made. As a result, EA was chosen as the most convenient and easy platform for third-party software implementations. The EA system is a rather cheap solution, known by many IT developers, which enables implementation of additional plug-ins in the form of DLL (Dynamic-Link Library) files. The EA system uses a database which is open and accessible to programmers so it is quite easy for them to build their own tables for the purposes of potential plug-ins. The EA producer also expressed preliminary agreement to offer the plug-in for their customers.

Firstly, the model of the plug-in was made in UML on the basis of functional requirements proposed by IT products developers. The database structure was modeled for the ST documents sections data. The toolbox of graphical objects for building elements of SPD and ST sections was worked out. The toolbox contains objects of assets, security objectives, assumptions, threats, security functions and requirements, and connectors for making relations between them. The objects have dialog windows which are connected to the knowledge base of the CCMODE Tools system. On that basis special wizards windows and inferring procedures were worked out.

Next these procedures use predefined ST elements stored in the knowledge base, e.g. assets types and forms with corresponding threats, threats and corresponding objectives, and objectives connected to predefined SFRs. The procedures use many other parameters of the objects, for instance: the form and type of assets which influence the type of adverse actions and possible vulnerabilities, value of assets, possible loss or the likelihood of a dangerous security incident. The knowledge base comprises the guidelines that help to resolve typical security problems with the use of predefined
security objectives, threats, assumptions, and security policies. The predefined elements of SPD and its solutions are connected by relations through the database in order to make the lists of proposed security objectives and SFRs shorter. These relations are the result of analyses made in the CCMODE project concerning dozens of STs and PPs, templates and guidelines describing how to define and solve the security problem. The last steps of the plug-in development process were verification and validation of a prototype software tool in some ST projects of IT devices.

The next section of the paper presents some final results of the plug-in application for elaborating the ST document of the chosen data diode (FFHDD).

3 Results of Plug-in Application

The plug-in tool was used for making the SPD section of ST for the chosen data diode. As a result, the graphical form of SPD and its solution (described in section 2.1 of this paper) were worked out (Fig. 1).

Figure 1 shows all major objects of the plug-in ST toolbox with their mutual relations: D – assets, S – entities using assets, T – threats, A – assumptions, O – security objectives for the TOE, OE – security objectives for the operational environment of the TOE, SFR – security functional requirement, and the blue line which groups the selected SFRs into one security function. This graphical form of ST is next automatically
pasted to the final ST document in another module of the CCMODE Tools system. This module is called documents generator and it uses the design pattern of ST.

4 Conclusions

This paper presented the software tool to support developers in elaborating the security problem definition – the most important part of the Security Target document. The plug-in tool was one of the results of the CCMODE R&D project. The tool is a part of the bigger CCMODE Tools system which fully supports security development and TOE development processes.

The paper presents general guidelines for the data diodes developers in accordance with the Common Criteria standard. It was noticed that some Polish developers might need to accredit similar devices according to the CC standard, that is why the data diode was used as an example. The paper provides developers with basic information about the security development process which can be supported by the plug-in application.

Therefore the plug-in software tool as well as the whole CCMODE Tools system are promising means for supporting developers of IT security enhanced products. The plug-in facilitates and speeds up the IT security development process and improves the quality of the ST document in the sections concerning security problem to be solved by the TOE. The objects used in the plug-in for one device can be reused in other projects of similar products. The developer gets a graphical picture of the security problem which is easy to analyze and to verify. The selection of security objectives and SFRs is supported by inferring wizards based on the knowledge base. Each step of SPD development can be checked and verified by the reports module of the plug-in. The reports consist of set of tables which have a similar role to rationale tables used in standard evidence documents but this the topic for the next paper.

Future work will be focused on building a standalone, independent plug-in application with its own database in order to separate it from the CCMODE Tools system. As a result the mobility of the plug-in can be improved and the costs of deployment and implementation can be reduced.

References

1. Fort Fox Hardware Data Diode, https://www.fox-it.com/en/products/datadiode
2. Filbico Data Diode, http://www.filbico.pl/index.php/pl/zno
3. Waterfall Security Solutions USA, http://www.waterfallsecurity.com/technology
4. Owl Computing Technologies, http://www.owlcti.com/dualdiode_technology.html
5. VS-diode, http://www.genua.eu/produkte/datendiode/index.en.html
6. Common Criteria for Information Technology Security Evaluation (Ver. 3.1, Revision 4) Part 1: Introduction and general model (ISO/IEC 15408-1) (September 2012)
7. Common Criteria for Information Technology Security Evaluation (Ver. 3.1, Revision 4) Part 2: Security functional requirements (ISO/IEC 15408-2) (September 2012)
8. Common Criteria for Information Technology Security Evaluation (Ver. 3.1, Revision 4) Part 3: Security assurance requirements (ISO/IEC 15408-3) (September 2012)
9. The Common Criteria Portal, http://www.commoncriteriaportal.org
10. Certification Report EAL4+ – NSCIB-CC-09-11025-CR, Fort Fox Hardware Data Diode, version FFHDD2+, TNO certification (September 3, 2009)
11. Certification Report EAL7+ – NSCIB-CC-09-11025-CR2, Fort Fox Hardware Data Diode, version FFHDD2+, TNO certification (June 16, 2010)
12. Common Methodology for Information Technology Security Evaluation (Version 3.1, Revision 4). Evaluation Methodology (September 2012)
13. Białas, A.: Patterns Improving the Common Criteria Compliant IT Security Development Process. In: Zamojski, W., Kacprzyk, J., Mazurkiewicz, J., Sugier, J., Walkowiak, T. (eds.) Dependable Computer Systems. AISC, vol. 97, pp. 1–16. Springer, Heidelberg (2011)
14. Rogowski, D., Nowak, P.: Pattern Based Support for Site Certification. In: Zamojski, W., Mazurkiewicz, J., Sugier, J., Walkowiak, T., Kacprzyk, J., et al. (eds.) Complex Systems and Dependability. AISC, vol. 170, pp. 179–193. Springer, Heidelberg (2012)
15. Białas, A. (ed.): Applying design patterns in security development process according to the Common Criteria standard. Original Polish title: Zastosowanie wzorców projektowych w konstruowaniu zabezpieczeń informatycznych zgodnych ze standardem Common Criteria. Wydawnictwo Instytutu Technik Innowacyjnych EMAG, financed by UE POIG 1.3.1, Katowice (2011) ISBN 978-83-932737-2-0
16. ISO/IEC TR 15446: Information technology – security techniques – guide for the production of Protection Profiles and Security Targets (2009)
17. BSI: The PP/ST guide, Version 1, Revision 6.2 (August 2007)
18. BSI: Guidelines for developer documentation according to CC Version 3.1 (2007)
19. BSI: Guidelines for evaluation reports according to Common Criteria Version 3.1, Version 2.00 for CCv3.1 rev. 3 (2010)
20. Higaki, W.H.: Successful Common Criteria evaluations. A practical guide for vendors. Create Space Independent Publishing Platform (2010)
21. Rogowski, D.: Computer-aided tool based on Common Criteria related design patterns. In: Korczak, J., Dudycz, H., Dyczkowski, M. (eds.) Business Informatics, vol. 3(29), pp. 111–127. Wrocław University of Economics Research Papers (2013)
22. CCMODE Project (Common Criteria compliant, Modular, Open IT security Development Environment), http://www.commoncriteriaportal.org/
23. Białas A.: Security-related design patterns for intelligent sensors requiring measurable assurance. Electrical Review (Przegląd Elektrotechniczny) 85(R.85(7)), 92–99 (2009) ISSN 0033-2097
24. Białas, A.: Common Criteria Related Security Design Patterns for Intelligent Sensors – Knowledge Engineering-Based Implementation. Sensors (August 2011)
25. Białas, A.: Ontological approach to the motion sensor security development. Electrical Review (Przegląd Elektrotechniczny) 85(R.85(11)), 36–44 (2009) ISSN 0033-2097
26. Białas, A.: Common Criteria Related Security Design Patterns – Validation on the Intelligent Sensor Example Designed for Mine Environment. Sensors (April 2010)
27. Białas, A.: How to develop a biometric system with claimed assurance. In: Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 775–780. IEEE Xplore Digital Library (2013)
28. Rogowski, D.: Software Implementation of Common Criteria Related Design Patterns. In: Proceedings of the 2013 Federated Conference on Computer Science and Information Systems (FedCSIS), Annals of Computer Science and Information Systems, pp. 1147–1152. IEEE Xplore Digital Library (2013)