dr inż. ANDRZEJ BIAŁAS
Instytut Technik Innowacyjnych EMAG

Informatyczne produkty sprzętowe, oprogramowanie oraz systemy o zadanym poziomie uzasadnionego zaufania

Hardware, software and systems with claimed assurance level

Artykuł dotyczy zagadnień związanych z konstruowaniem i oceną zabezpieczeń wbudowywanych w dowolne produkty lub systemy informatyczne. Zabezpieczenia te dotyczą funkcji użytkowych i powinny się cechować tak zwanym uzasadnionym zaufaniem, utożsamianym potocznie z wiarygodnością. Przedstawiona w artykule metodyka Common Criteria, opisana w standardzie ISO/IEC 15408, jest podstawową metodyką kreowania uzasadnionego zaufania dla zabezpieczeń informatycznych. Metodyka obejmuje trzy główne procesy. W procesie konstruowania zabezpieczeń, na podstawie różnego typu analiz bezpieczeństwa, wypracowywany jest specjalny dokument zwany zadaniem zabezpieczeń, który stanowi zbiór wymagań bezpieczeństwa – funkcjonalnych (jak zabezpieczenia mają działać) i uzasadniających zaufanie (jaką wiarygodnością mają być one obdarzane). Drugi proces dotyczy konstruowania produktu lub systemu informatycznego oraz opracowania jego dokumentacji, która stanowi rozwinięcie wspomnianego zadania zabezpieczeń. Dokumentacja ta pełni rolę materiału dowodowego w trzecim procesie – w procesie niezależnej oceny zabezpieczeń, który powinien doprowadzić do uzyskania certyfikatu. Dzięki zastosowanemu rygorowi konstruowania oraz niezależnej i wnikliwej ocenie, produkty certyfikowane są uznawane za bardziej wiarygodne, a przez to szczególnie predysponowane do zastosowań obarczonych podwyższonym poziomem ryzyka.

The paper deals with the issues related to the development and evaluation of security functions embedded into IT products and systems. These functions relate to utility functions of the products or systems and should have the so called assurance, commonly understood as reliability. The Common Criteria methodology presented in this paper, described in the ISO/IEC 15408 standard, is the basic methodology to create assurance for IT security. The methodology comprises three major processes. During the security development process, based on different types of security analyses, a document called Security Target is developed. This document is a set of security requirements – functional requirements (how the security functions should work) and assurance requirements (what their reliability should be like). The second process is related to the development of an IT product or system, along with documentation which is a supplement to the above mentioned Security Target. The documentation serves as evidence material in the third process – the process of independent security evaluation which should lead to obtaining a certificate. Thanks to the applied development rigour, as well as independent and thorough evaluation, certified products are recognized as more reliable, thus especially predisposed for high-risk applications.

1. WSTĘP

Metodyka Common Criteria (CC), dostępna obecnie w wersji CC 3.1, opisana w standardzie ISO/IEC 15408

1. INTRODUCTION

The Common Criteria (CC) methodology, currently available in CC 3.1 version, described in the ISO/IEC

[1], [2], [3], jest podstawową metodyką kreowania uzasadnionego zaufania dla „produktów i systemów informatycznych", które w nomenklaturze standardu określane są jako „przedmiot oceny" (ang. *TOE – Target of Evaluation*). Przedmiotem oceny może być sprzęt informatyczny, w tym inteligentne urządzenia elektroniczne, oprogramowanie, w tym układowe oraz zbudowane z nich systemy. Istotną kwestią jest to, by występowały w nich zabezpieczenia funkcji użytkowych. Zabezpieczenia powinny cechować się tak zwanym uzasadnionym zaufaniem (*ang. assurance*), określanym tu jako „przekonanie, że przedmiot oceny, czyli TOE spełnia wyspecyfikowane cele zabezpieczeń". „Przekonanie" to nie może być bezkrytyczne, lecz oparte na pewnych dowodach, eksperymentach. Musi bowiem istnieć jakaś podstawa zaufania, że w sytuacji kryzysowej związanej z wystąpieniem określonego zagrożenia, zabezpieczenia, czyli funkcje zabezpieczające TOE (ang. *TSF – TOE Security Functions*) rzeczywiście zadziałają. Przyjęto, że źródłem uzasadnionego zaufania jest rygorystyczny proces konstruowania, wytwarzania i utrzymywania produktu lub systemu, a także proces niezależnej oceny (stąd określenie „przedmiot oceny"), prowadzonej w akredytowanym laboratorium. Uzasadnione zaufanie jest mierzalne w skali EAL (ang. *Evaluation Assurance Level*): od EAL1 (min.) do EAL7 (max.).

Powszechnie uważa się, że certyfikowane produkty lub systemy informatyczne są przeznaczone głównie do najbardziej odpowiedzialnych zastosowań, zwłaszcza tam, gdzie występuje zwiększony poziom ryzyka, przetwarzane są zasoby informacji o dużym znaczeniu lub świadczone są usługi o charakterze krytycznym. W sektorze górnictwa może to dotyczyć na przykład: systemów informatycznych wykorzystywanych do zarządzania procesami biznesowymi, systemów nadzorujących procesy produkcyjne i bezpieczeństwo załogi, a także wielu inteligentnych urządzeń elektronicznych decydujących o bezpieczeństwie, w tym różnego typu czujników.

Artykuł zawiera wprowadzenie do metodyki Common Criteria i na tym tle prezentuje trzy jej podstawowe procesy:

- proces konstruowania zabezpieczeń (ang. *IT security development*),
- proces konstruowania produktu lub systemu (ang. *TOE development*),
- proces oceny zabezpieczeń (ang. *IT security evaluation*).

Artykuł ma na celu przybliżenie informatykom, elektronikom i menadżerom zagadnień związanych z konstruowaniem, wytwarzaniem oraz stosowaniem certyfikowanych produktów lub systemów informatycznych.

15408 standard [1], [2], [3], is the basic methodology to create assurance for IT products and systems which, according to CC definitions, are identified as TOE – Target of Evaluation. The TOE can be hardware, including intelligent electronic devices; or software, including software systems. An important issue is that utility functions of these systems should be secure. This security should have the so called assurance which is understood here as "confidence that the TOE meets security requirements specified for it". This confidence cannot be uncritical. It has to be based on certain evidences or experiments. There must be a basis for confidence that in an emergency, resulting from a certain threat, the TOE security functions (TSF) will really work. It was assumed that the basis of assurances is a rigorous process of developing, producing and maintaining an IT product or system, as well as an independent evaluation process (thus the name „target of evaluation") carried out in an accredited laboratory. Assurance is measurable in the EAL (Evaluation Assurance Level) scale: from EAL1 (minimum) to EAL7 (maximum).

It is commonly acknowledged that certified products or systems are used mainly in the most responsible applications, especially those with a higher risk level, those which process high-importance data assets or perform critical services. In the mining sector this may relate to, for example: IT systems used for the management of business processes, systems for the supervision of production processes and personnel safety, as well as many safety-oriented intelligent electronic devices, including different types of sensors.

The paper comprises an introduction to the Common Criteria methodology and, against this background, presents three basic processes of this methodology:

- IT security development,
- TOE development,
- IT security evaluation.

The objective of the paper is to make IT engineers, electronics engineers and managers familiar with the issues related to the development, production and use of certified IT products or systems.

2. WPROWADZENIE DO ZAGADNIEŃ ZAWARTYCH W STANDARDZIE

Standard *Common Criteria for Information Security Evaluation* (Wspólne kryteria do oceny zabezpieczeń informatycznych) jest ogólnie dostępny na portalu Common Criteria [4]. Składa się on z trzech części:

- *ISO/IEC 15408-1 (CC Part 1)* zawiera: wprowadzenie, opis modelu zarządzania ryzykiem i kreowania uzasadnionego zaufania oraz struktur podstawowych dokumentów, opracowywanych na potrzeby certyfikacji produktu lub systemu, tj.: zadania zabezpieczeń (ang. *ST – Security Target*) i profilu zabezpieczeń (ang. *PP – Protection Profile*), a także ich uproszczonych wersji (ang. *low assurance ST/PP*) stosowanych dla EAL1;
- *ISO/IEC 15408-2 (CC Part 2)* zawiera katalog komponentów funkcjonalnych (ang. *functional components*) służących do modelowania funkcjonalnych wymagań bezpieczeństwa (ang. *SFR – Security Functional Requirements*), czyli wymagań stawianych funkcjom zabezpieczającym;
- *ISO/IEC 15408-3 (CC Part 3)* zawiera katalog komponentów uzasadniających zaufanie (ang. *assurance components*), służących do modelowania wymagań uzasadniających zaufanie do funkcji zabezpieczających (ang. *SAR – Security Assurance Requirements*);

Proces konstruowania zabezpieczeń opisano w przewodniku [5]. Dla specjalistów zajmujących się oceną zabezpieczeń podstawowym dokumentem jest metodyka oceny CEM [6].

Komponenty funkcjonalne zostały podzielone tematycznie na 11 klas (Tabela 1); każda klasa dzieli się na rodziny, zaś dana rodzina zawiera komponenty precyzujące dane zagadnienie bezpieczeństwa. Komponenty składają się z elementów, które szczegółowo prezentują dane zagadnienie bezpieczeństwa.

Przykład 1: Komponent funkcjonalny *FCS_COP.1 Cryptographic operations*, należy do rodziny *FCS_COP* wchodzącej w skład klasy *FCS*. Komponent ten służy do wyspecyfikowania operacji kryptograficznej, wskazując: rodzaj operacji (szyfrowanie, odszyfrowanie, realizację funkcji skrótu, itp.), stosowany algorytm (na przykład *DES – DataEncryption Standard*), długość klucza kryptograficznego (np. 168 bitów) oraz nazwę standardu specyfikującego szczegóły tego algorytmu (np.: FIPS PUB 46).

2. INTRODUCTION TO THE ISSUES INCLUDED IN THE STANDARD

The Common Criteria for Information Technology Security Evaluation standard is available free of charge from the Common Criteria portal [4]. The standard consists of three parts:

- *ISO/IEC 15408-1 (CC Part 1)* includes the following: introduction, terms, general model, structures of basic documents worked out for the purposes of IT product or system certification, i.e. ST – Security Target and PP – Protection Profile, along with their simplified versions – low assurance ST/PP used for EAL1;
- *ISO/IEC 15408-2 (CC Part 2)* includes a catalogue of functional components used for modelling Security Functional Requirements (SFR);
- *ISO/IEC 15408-3 (CC Part 3)* includes a catalogue of assurance components used for modelling Security Assurance Requirements (SAR).

The process of IT security development is described in a guide [5]. The basic document for security evaluators is Common Methodology for Information Technology Security Evaluation (CEM) [6].

Functional components were divided into 11 classes (Table 1), and the classes into families, while a given family comprises components which refer to certain security issues. The components consist of elements which present the given issue in details.

Example 1: The *FCS_COP.1 Cryptographic operations* functional component belongs to the *FCS_COP* family which is a part of the *FCS* class. This component serves to specify cryptographic operations and indicates: type of operation (encryption, decryption, hashing function, etc.), used algorithm (for *DES – Data Encryption Standard*), length of cryptographic key (e.g. 168 bits), and the name of the standard specifying the details of this algorithm (e.g. FIPS PUB 46).

Tabela 1/Table 1

Klasy komponentów funkcjonalnych [2]
Functional components classes [2]

Klasa Class	Nazwa klasy Class name
FAU	Audyt bezpieczeństwa Security Audit
FCO	Transmisja Communication
FCS	Ochrona kryptograficzna Cryptographic Support
FDP	Ochrona danych użytkownika User Data Protection
FIA	Identyfikacja i uwierzytelnianie Identification and Authentication
FMT	Zarządzanie bezpieczeństwem Security Management
FPR	Prywatność Privacy
FPT	Ochrona funkcji zabezpieczających Protection of the TSF
FRU	Wykorzystanie zasobów Resource Utilization
FTA	Dostęp do TOE TOE Access
FTP	Wiarygodne ścieżki i kanały Trusted path/channels

Tabela 2/Table 2

Klasy komponentów uzasadniających zaufanie [3]
Assurance components classes [3]

Klasa Class	Nazwa klasy Class name
APE	Ocena dokumentu PP Protection Profile Evaluation
ASE	Ocena dokumentu ST Security Target Evaluation
ADV	Prace badawcze i rozwojowe Development
AGD	Dokumentacja Guidance Documents
ALC	Wsparcie cyklu życia produktu Life-Cycle Support
ATE	Testowanie Tests
AVA	Oszacowanie podatności Vulnerability Assessment
ACO	Systemy złożone Composition

Podobną strukturę przyjęto dla komponentów uzasadniających zaufanie. Zostały one tematycznie podzielone na 8 klas (Tabela 2). Każda klasa dzieli się na rodziny, zaś w danej rodzinie występują komponenty, wyrażające elementarne zagadnienia dotyczące tworzenia podstaw zaufania. W rodzinie są one uporządkowane hierarchicznie, według narastającego i kumulowanego rygoru.

A similar structure was adopted for assurance components. They were divided into 8 classes (Table 2). Each class consists of families, while in each family there are components expressing elementary issues of the assurance basis development. In a family they are arranged according to increasing and accumulating rigour.

Komponenty uzasadniające zaufanie mają również swoje elementy, przy czym mogą być one trzech rodzajów:
- element D określa, jaki artefakt (dowód na spełnienie wymagania wyrażonego przez komponent) konstruktor powinien dostarczyć, na przykład przedłożyć wyniki pewnej analizy, opracować pewien dokument lub jego część,
- element C określa, jaką postać powinien mieć ten artefakt i co ma on zawierać,
- element E określa, w jaki sposób dostarczony artefakt o danej postaci będzie sprawdzany przez oceniającego.

Przykład 2: Komponent funkcjonalny *ATE_DPT.2 Testing: security enforcing module* (testowanie na poziomie modułów odpowiedzialnych za realizację (wymuszanie) funkcji zabezpieczających), należy do rodziny *ATE_DPT* wchodzącej w skład klasy *ATE*.

Założono tu, że przedmiot oceny zdekomponowano na podsystemy, te zaś na moduły. Część z tych modułów jest związana z realizacją funkcji zabezpieczających (reprezentuje zabezpieczenia). Dla tego typu modułów konstruktor powinien przedstawić dowód na to, że zostaną one w pełni i właściwie przetestowane. Dowód może mieć postać tabeli pokrycia testami poszczególnych modułów.

Należy zwrócić uwagę, że w Tabeli 2 występują trzy rodzaje klas, różniące się swym przeznaczeniem. Do TOE bezpośrednio odnoszą się klasy dotyczące prac rozwojowych (ADV), dokumentacji użytkowej (AGD), cyklu życia (ALC), testowania (ATE) oraz analizy podatności (AVA).

Klasy ASE i APE określają odpowiednio wymagania na postać dokumentu zadania zabezpieczeń lub profilu zabezpieczeń. Wymagania zawarte w klasie ACO przedstawiają, jak konstruować złożone przedmioty oceny, w skład których wchodzą informatyczne produkty lub systemy, które zostały wcześniej ocenione i uzyskały stosowne certyfikaty.

Znaczenie poziomów, czyli miar uzasadnionego zaufania jest interpretowane w sposób następujący:
- EAL1 – określa, że „TOE był testowany funkcjonalnie" (ang. *functionally tested*),
- EAL2 – określa, że „TOE był testowany strukturalnie" (ang. *structurally tested*),
- EAL3 – określa, że „projekt TOE był metodycznie sprawdzany i testowany" (ang. *methodically tested and checked*),
- EAL4 – określa, że „TOE był metodycznie projektowany, testowany i przeglądany" (ang. *methodically designed, tested and reviewed*),
- EAL5 – określa, że „TOE był półformalnie projektowany i testowany" (ang. *semiformally designed and tested*),

Assurance components can have three kinds of elements:
- D element indicates which artifact (evidence that a given requirement expressed by the component has been fulfilled) the developer should provide, for example, submit the results of an analysis, prepare a document or its part,
- C element indicates the form and contents of the artifact,
- E element indicates how the provided artifact, in a given form, will be checked by the evaluator.

Example 2: The *ATE_DPT.2 Testing: security enforcing module* functional component belongs to the *ATE_DPT* family which is a part of the *ATE* class.

Here it was assumed that the Target of Evaluation (TOE) had been decomposed into subsystems which, in turn, had been decomposed into modules. A part of these modules is related to security functions (represents security). For this type of modules the developer should provide evidence that they will be completely and properly tested. The evidence can have a form of a table showing how particular modules are covered by tests.

Please note that there are three types of classes in Table 2, with different purposes. The ADV classes relate directly to the TOE, AGD to guidance documents, ALC to life-cycle support, ATE to tests, and AVA to vulnerability assessment.

The ASE and APE classes determine the requirements for the Security Target document or Protection Profile document respectively. The requirements included in the ACO class present how to construct complex protection profiles, comprising IT products or systems which were evaluated earlier and were granted suitable certificates.

Evaluation Assurance Levels are interpreted as follows:
- EAL1 – means that the TOE was functionally tested,
- EAL2 – means that the TOE was structurally tested,
- EAL3 – means that the TOE project was methodically tested and checked,
- EAL4 – means that the TOE was methodically designed, tested and reviewed,
- EAL5 – means that the TOE was semiformally designed and tested,

- EAL6 – określa, że „projekt TOE został półformalnie zweryfikowany i przetestowany" (ang. *semi-formally verified design and tested*),

- EAL7 – określa, że „projekt TOE został formalnie zweryfikowany i przetestowany" (ang. *formally verified design and tested*).

Należy nadmienić, że określenie „nieformalny" (ang. *informal*) rozumiane jest w standardzie jako „wyrażony w języku naturalnym", określenie „półformalny" (ang. *semiformal*) rozumiane jest jako „wyrażony w języku o ściśle zdefiniowanej składni i zdefiniowanej semantyce", zaś określenie „formalny" (ang. *formal*) rozumiane jest jako „wyrażony w języku o ściśle zdefiniowanej składni oraz semantyce, która jest oparta na solidnych podstawach matematycznych".

Deklarowanym przez konstruktorów poziomom uzasadnionego zaufania dla TOE odpowiadają specjalnie skomponowane zbiory komponentów uzasadniających zaufanie, zwane pakietami, przedstawione w tabeli 1 zamieszczonej w trzeciej części standardu [3]. Na jej podstawie opracowano Tabelę 3, ale zamieszczono w niej jedynie komponenty dotyczące TOE. Wiersze tej tabeli reprezentują komponenty z poszczególnych rodzin wchodzące w skład pakietów EAL, a samym pakietom odpowiadają kolumny.

Rodzina ADV_ARC, dotycząca architektury TOE zawiera tylko jeden komponent ADV_ARC.1 uwzględniany począwszy od EAL2. Rodzina ADV_FSP posiada sześć komponentów: ADV_FSP.1, ADV_FSP.2, ADV_FSP.3, ADV_FSP.4, ADV_FSP.5 oraz ADV_FSP.6, przy czym ADV_FSP. wchodzi w skład zarówno EAL5, jak i EAL6. Reguły te dotyczą wszystkich pozostałych rodzin komponentów: ADV_IMP (reprezentacja implementacji), ADV_INT (wewnętrzna struktura funkcji zabezpieczających), ADV_SPM (model polityki bezpieczeństwa), ADV_TDS (projekt TOE – dekompozycja na podsystemy i moduły), AGD_OPE (dokumentacja użytkowa), AGD_PRE (procedury przygotowawcze – instalacji i uruchomienia), ALC_CMC (możliwości techniczno-organizacyjne systemu zarządzania konfiguracją), ALC_CMS (zakres zarządzania konfiguracją, listy konfiguracyjne TOE i ich elementy), ALC_DEL (procedury dostawy), ALC_DVS (bezpieczeństwo środowiska rozwojowego TOE), ALC_FLR (proces zarządzania usuwaniem usterek), ALC_LCD (zdefiniowanie modelu cyklu życia dla TOE), ALC_TAT (narzędzia stosowane przez konstruktorów), ATE_COV (pokrycie TOE testami), ATE_DPT (głębokość testowania), ATE_FUN (testy funkcjonalne), ATE_IND (niezależne testy prowadzone przez oceniających) oraz AVA_VAN (analiza podatności).

- EAL6 – means that the TOE project was semiformally verified design and tested,

- EAL7 – means that the TOE project was formally verified design and tested.

It is important to note that "informal" is understood in the standard as "expressed in natural language", "semiformal" is understood as "expressed in a restricted syntax language with defined semantics", and "formal" – "expressed in a restricted syntax language with defined semantics based on well-established mathematical concepts".

Evaluation assurances levels for the TOE declared by the developers refer to specially composed sets of assurance components, called packages, presented in Table 1 in the third part of the standard [3]. This was the basis for Table 3 prepared for this paper, however, the table has only the TOE-related components. The rows of the table represent components from particular families, included in EAL packages, while columns represent the packages themselves.

The ADV_ARC, family refers to the TOE architecture and has only one component ADV_ARC.1 considered from EAL2 upwards. The ADV_FSP family has six components: ADV_FSP.1, ADV_FSP.2, ADV_FSP.3, ADV_FSP.4, ADV_FSP.5, and ADV_FSP.6, however ADV_FSP.5 is a part of both EAL5 and EAL6. These rules are valid for all remaining component families: ADV_IMP (implementation representation), ADV_INT (TSF internals), ADV_SPM (security policy model), ADV_TDS (TOE Design – basic modular design), AGD_OPE (operational user guidance), AGD_PRE (preparative procedures – installation and start-up), ALC_CMC (configuration management capabilities), ALC_CMS (configuration management scope – TOE configuration lists and their elements), ALC_DEL (delivery procedures), ALC_DVS (TOE development security), ALC_FLR (flaw remediation), ALC_LCD (life-cycle definition for the TOE), ALC_TAT (tools and techniques applied by the developers), ATE_COV (test coverage), ATE_DPT (depth of testing), ATE_FUN (functional tests), ATE_IND (independent testing carried out by evaluators), and AVA_VAN (vulnerability analysis).

Tabela 3/Table 3

Komponenty uzasadniające zaufanie wchodzące w skład poszczególnych pakietów EAL (pominięto klasy APE i ASE) – wytłuszczono numery komponentów pojawiające się po raz pierwszy lub zastępujące komponenty o mniejszym rygoryzmie [3]

Assurance components included in particular EAL packages (APE and ASE classes are omitted) – the numbers of components which appear for the first time or replace components with lower rigour are in bold [3]

Klasa Class	Rodzina Family	Poziom uzasadnionego zaufania Assurance level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
ADV	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
AGD	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
ALC	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR	Opcjonalne dla dowolnego EAL Optionally for any EAL						
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
ATE	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	**2**	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
AVA	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5

Kolumny Tabeli 3 reprezentują komponenty wchodzące w skład poszczególnych pakietów EAL. Na przykład EAL 3 zawiera następujące komponenty: ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1, AGD_PRE.1, ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2 i AVA_VAN.2.

Im wyższy EAL, tym więcej zawiera on komponentów i tym bardziej są one rygorystyczne (zawierają więcej elementów, reprezentujących ich rygor). Produkty lub systemy informatyczne o wyższym EAL są obdarzane większym zaufaniem, jednak koszt ich opracowania i oceny znacząco rośnie, stąd deklarując EAL, należy kierować się pewnym kompromisem.

3. PROCES KONSTRUOWANIA ZABEZPIECZEŃ PRODUKTÓW LUB SYSTEMÓW INFORMATYCZNYCH

Typową ścieżką postępowania podczas konstruowania, jest opracowanie zadania zabezpieczeń (ST) na podstawie analizy wymagań użytkowych i środo-

The columns of Table 3 represent components which are part of particular EAL packages. For ex ample, EAL3 contains the following components: ADV_ARC.1, ADV_FSP.3, ADV_TDS.2, AGD_OPE.1, AGD_PRE.1, ALC_CMC.3, ALC_CMS.3, ALC_DEL.1, ALC_DVS.1, ALC_LCD.1, ATE_COV.2, ATE_DPT.1, ATE_FUN.1, ATE_IND.2, and AVA_VAN.2.

The higher the EAL is, the more components it has and the more rigorous these components are (they contain more elements representing their rigour). IT products or systems with a higher EAL have a higher assurance level. however the cost of their development and evaluation is significantly higher too. Therefore, while declaring an EAL, it is necessary to compromise.

3. IT PRODUCTS OR SYSTEMS SECURITY DEVELOPMENT PROCESS

A typical path to take during the security development process is to work out a Security Target based on the analysis of operational and environment re-

wiskowych dotyczących TOE (alternatywą ścieżką jest opracowanie ST na podstawie wcześniej opracowanego i ocenionego profilu zabezpieczeń). Proces konstruowania zabezpieczeń sprowadza się do wypełnienia treścią struktury dokumentu ST zdefiniowanego w załączniku (normatywnym) do [1] i obejmuje następujące etapy:

1. Przeprowadzenie analizy wymagań użytkowych i środowiskowych dotyczących produktu lub systemu informatycznego i na tej podstawie opracowanie sekcji ST zatytułowanej „Wprowadzenie do zadania zabezpieczeń" (*ang. ST Introduction*). Poza identyfikatorami zadania zabezpieczeń i samego przedmiotu oceny, sekcja ta zawiera: zwięzły opis tworzonego produktu lub systemu informatycznego, jego środowiska rozwoju, produkcji i eksploatacji, elementy składowe i sposób wykorzystania.
2. Sformułowanie deklaracji zgodności (ang. *Conformance claims*). Dotyczy to stosowanej wersji standardu (aktualnie jest nią wersja CC 3.1), deklarowanej zgodności z profilami zabezpieczeń (ocenionymi zbiorami wymagań do wielokrotnego zastosowania) i z zadeklarowanym pakietem EALn, czasem z EALn+. Plus oznacza tu, że do standardowego pakietu EAL dodano jakiś komponent lub pewien jego komponent zastąpiono innym z danej rodziny, ale o wyższym rygoryzmie.
3. Opracowanie definicji problemu bezpieczeństwa dla TOE (ang. *Security problem definition*; do wersji 2.x standardu stosowano określenie „otoczenie zabezpieczeń" – ang. *Security environment*). Obejmuje to identyfikację zagrożeń dla TOE i jego otoczenia, określenie zasad polityki bezpieczeństwa dla TOE oraz przyjęcie założeń odnoszących się do środowiska rozwoju, produkcji i eksploatacji.
4. Na podstawie analizy problemu bezpieczeństwa stawiane są cele bezpieczeństwa (ang. *Security objectives*) dla TOE oraz jego środowisk (rozwoju, produkcji i eksploatacji). Cele stanowią rozwiązanie zidentyfikowanego problemu bezpieczeństwa. Ponadto należy uzasadnić, że wobec wszystkich zagrożeń podjęto środki zaradcze, wszystkie zasady polityki bezpieczeństwa będą wymuszane, zaś przyjęte założenia będą podtrzymywane (właśnie przez wyspecyfikowanie odpowiednich celów środowiskowych).
5. Wprowadzenie definicji komponentów dodatkowych, jednak w swej postaci zgodnych z przyjętą w Common Criteria konwencją (ang. *Extended components definition*). Sytuacja taka występuje dość rzadko. Dzieje się to wówczas, gdy żaden z komponentów opisanych w standardzie [2], [3] nie jest w stanie wyrazić specyficznych potrzeb konstruktora. Na przykład, dla aplikacji generujących

requirements for the TOE (an alternative is to work out the ST on the basis of previously developed and evaluated Protection Profile). The security development process is thus reduced to providing contents to the ST document defined in the normative attachment to [1]. The process comprises the following stages:

1. The analysis of functional and environment requirements related to an IT product or system. This is the basis to work out the ST Introduction. Apart from the ST and the TOE identifiers, the section contains: a short overview of the developed IT product or system, its development environment, production and exploitation, elements, and application.
2. Formulating Conformance Claims. This refers to the current version of the standard (CC 3.1), declared conformance to Protection Profiles (evaluated sets of requirements for multiple use), and the declared EALn package, sometimes EALn+. The plus means that a component was added to the standard EAL package, or a component of this package was replaced by another from the given family but of a higher rigour.
3. Working out a security problem definition for the TOE (in the previous versions of the standard – till CC 2.x – the term "Security environment" was used). This comprises the identification of threats for the TOE and its environment, determining security policy rules for the TOE, and setting assumptions for development, production and exploitation environments.
4. Based on the analysis of the security problem, the security objectives are determined for the TOE and its environments (development, production and exploitation). The objectives are a solution to the identified security problem. Additionally, it is necessary to justify that there are measures taken with respect to all threats, all security policy rules will be enforced, while the declared assumptions will be upheld (through the specification of environmental objectives).
5. Extended Components Definition, according to the convention used in the Common Criteria standard. This situation is very unlikely. It happens so when not a single component described in the standard [2], [3] is able to express specific needs of the developer. For example, in the case of applications generating cryptographic keys there is a functional component defined which expresses the quality of random numbers (their entropy), and the standard does not include this component.

klucze kryptograficzne, zostaje definiowany komponent funkcjonalny określający jakość liczb losowych (ich entropię), którego standard nie zawiera.

6. Wypracowanie i uzasadnienie specyfikacji wymagań bezpieczeństwa (*ang. SFR – Security functional requirements* oraz *SAR – Security assurance requirements*). Sprowadza się to do wyrażenia celów bezpieczeństwa podanych dla TOE za pomocą funkcjonalnych wymagań bezpieczeństwa (SFR), czyli zastosowania komponentów funkcjonalnych [2]. Są to wymagania wobec funkcji zabezpieczających wbudowywanych do TOE. Podobnie specyfikuje się wymagania uzasadniające zaufanie (SAR) do tych funkcji. Wykorzystywane są wówczas komponenty uzasadniające zaufanie [3], wynikające z zadeklarowanego dla TOE poziomu EALn, czasem zastępowane komponentami o wyższym rygorze albo uzupełniane komponentami spoza pakietu EALn, co jest oznaczane, jak już wspomniano, jako EALn+. Podczas uzasadnienia przyjęto zasadę (dla każdego celu dla TOE), że jeśli wszystkie wymagania SFR odnoszące się do danego celu są spełnione, to ten cel zostanie osiągnięty i w rezultacie TOE będzie właściwie chroniony przed zagrożeniem i/lub reguła polityki zostanie wymuszona i/lub założenie będzie podtrzymane.
7. Ostatni etap opracowania zadania zabezpieczeń ma związek z implementacją wymagań bezpieczeństwa w postaci funkcji zabezpieczających TOE, czyli tak zwanych TSF. Zbiór tych zdefiniowanych funkcji określany jest mianem specyfikacji końcowej TOE (ang. *TSS – TOE summary specification*). Każda z funkcji jest związana określonym podzbiorem wymagań typu SFR i wyraża pewien zbiór możliwych do wykonania operacji.

W pewnym uproszczeniu można przyjąć, że funkcje to „czarne skrzynki" wyposażone w interfejsy. Takie podejście ułatwia realizację opisywanego dalej procesu konstruowania TOE, w którym te czarne skrzynki zostaną zdekomponowane na podsystemy, a te na moduły (kategorii: wymuszające funkcje zabezpieczające, wspomagające je w tym, nieistotne), zaś interfejsy zostaną uszczegółowione. Funkcje, wchodzące w skład specyfikacji TSS, zdefiniowane na bardzo ogólnym poziomie abstrakcji pokazują, w jaki sposób poszczególne wymagania będą implementowane. Na przykład, komponent *FTP_ITC.1 Inter-TSF trusted channel* dotyczący wymagań na szyfrowane kanały wymiany informacji odnosi się na przykład do funkcji o nazwie „*TrustedChannel*" zdefiniowanej przez konstruktora, która implementuje to wymaganie (wspomagane zwykle kilkoma innymi SFR, tu: dotyczącymi operacji kryptograficznych

6. Working out and providing rationale for security functional requirements (SFR) and security assurance requirements (SAR). This is reduced to the expression of security objectives given for the TOE by means of security functional requirements (SFR), i.e. the use of functional components [2]. These are requirements for security functions embedded in the TOE. Security assurance requirements (SAR) for these functions are specified in a similar way. In this situation assurance components are used [3], resulting from the EAL declared for the TOE, sometimes replaced by higher-rigour components or supplemented with components beyond the EALn package, which is marked as EALn+. During the rationale the following was assumed (for each objective for the TOE): if all security functional requirements referring to a given objective are fulfilled, the objective will be achieved and, as a result, the TOE will be properly protected against threats and/or the policy rule will be enforced and/or the assumption will be upheld.

7. The last stage of the Security Target development is related to the implementation of security objectives in the form of TOE security functions. The set of these defined functions is called TOE summary specification (TSS). Each function is related to a particular subset of security functions requirements (SFR) and expresses a set of operations that are possible to perform.

To make things easier, one can assume that the functions are "black boxes" equipped with interfaces. Such an approach facilitates the process of TOE construction which will be described further on. During this process the black boxes will be decomposed into subsystems which, in turn, will be decomposed into models (categories: modules enforcing security functions, models supporting this process, not applicable models), while interfaces will be specified. The functions which are part of the TSS specification, defined on a very general abstraction level, demonstrate how particular requirements will be implemented. For ex ample, the *FTP_ITC.1 Inter-TSF trusted channel* component about the requirements for data exchange encrypted channel refers to the „*TrustedChannel*" developer-defined function which implements this requirement (usually supported by several other SFRs, here: those referring to cryptographic operations and key management: *FCS_COP.1 Cryptographic operation*, *FCS_CKM.1 Cryptographic key generation*, *FCS_CKM.2 Cryptographic key distribution*, *FCS_CKM.4 Cryptographic key destruction*).

i zarządzania kluczami: *FCS_COP.1 Cryptographic operation*, *FCS_CKM.1 Cryptographic key generation*, *FCS_CKM.2 Cryptographic key distribution*, *FCS_CKM.4 Cryptographic key destruction*).

Wypracowanie profilu zabezpieczeń przebiega podobnie, jednak kończy się na etapie 6, gdyż profil nie odnosi się do sposobu implementacji wymagań w postaci funkcji zabezpieczających. Według ocenionego profilu, odpowiadającego rodzinie produktów lub systemów informatycznych o tych samych wymaganiach bezpieczeństwa, można tworzyć różne zadania zabezpieczeń i dalej według nich je konstruować. Wówczas takie zadanie zabezpieczeń ma uproszczoną postać i sprowadza się do zadeklarowania zgodności z profilem oraz wypracowaniu specyfikacji funkcji zabezpieczających (punkt 7) według wymagań zawartych w profilu. Często ze względów oszczędnościowych lub standaryzacyjnych, profile są opracowywane przez daną grupę producentów, nawet silnie konkurujących między sobą (na przykład dostawców kart kryptograficznych). Na podstawie opracowanego i ocenionego wspólnym wysiłkiem profilu, poszczególni producenci opracowują własne zadania zabezpieczeń, konstruują według nich produkty, certyfikują je i dalej konkurują.

4. PROCES KONSTRUOWANIA PRODUKTÓW LUB SYSTEMÓW INFORMATYCZNYCH WEDŁUG STANDARDU COMMON CRITERIA

W wyniku realizacji przedstawionego powyżej procesu konstruowania zabezpieczeń uzyskuje się dokument zadania zabezpieczeń, zawierający zbiór funkcji zabezpieczających odpowiadających określonym podzbiorom wymagań funkcjonalnych (SFR), które teraz należy zaimplementować w przyjętej technologii i na zadanym poziomie uzasadnionego zaufania EAL. Należy zauważyć, że ten sam zbiór funkcji zabezpieczających można implementować na różnym poziomie EAL. Zależy to od potrzeb, rodzaju zastosowań, przewidywanego tam ryzyka, wartości chronionych zasobów oraz samych możliwości finansowych twórców i producentów TOE. Niezależnie od zadeklarowanego EAL, proces konstruowania produktów lub systemów informatycznych przebiega podobnie, natomiast od poziomu EAL zależy jego szczegółowość i zakres działań. W toku procesu konstruowania, który ogólnie ma charakter zstępujący (ang. *top-down*), powstaje TOE (sprzęt informatyczny, oprogramowanie, w tym sprzętowe, systemy informa-

Working out a protection profile has a similar course, however it is completed at stage 6 as the profile does not refer to the method of requirements implementation in the form of security functions. A protection profile which refers to a family of IT products or systems with the same security requirements can be the basis to construct different security targets and develop them according to these requirements. Then such a security target has a simplified form and is reduced to the declared conformance with the profile and to working out the specification of security functions (item 7), according to the requirements included in the profile. Due to economical or standardization reasons, profiles are often developed by a group of producers who compete with one another (for example the providers of cryptographic cards). Based on the profile, developed and evaluated as a result of the group effort, particular producers work out their own security targets, develop products on their basis, certify them, and then compete with one another again.

4. IT PRODUCT OR SYSTEM DEVELOPMENT ACCORDING TO COMMON CRITERIA

As a result of the above described IT security development process, a security target document is worked out. The document contains a set of security functions which refer to particular subsets of security functional requirements (SFR). These SFRs must be now implemented according to the selected technology and at the claimed evaluation assurances level (EAL). It is important to note that the same set of security functions can be implemented at different EALs. It depends on the needs, type of application, expected risk, value of protected assets, and financial standing of the TOE developers and producers. No matter what the declared EAL is like, the process of IT products or systems development is similar. Still, the claimed EAL is decisive as far as the level of details and the operations range are concerned. During the development process, which is a top-down one, the TOE is made (hardware, software, IT systems) along with documentation which should have a special form compliant with the security assurance

tyczne) oraz tworzona jest jego dokumentacja, która powinna mieć specjalną postać, wynikającą z treści wymagań typu SAR zawartych w zadeklarowanym pakiecie EALn (czasem zmodyfikowanym do EALn+). Dokumentacja ta pełni rolę tak zwanego materiału dowodowego (ang. *evidences*), który razem z TOE jest przedkładany do niezależnej oceny.

Materiał dowodowy może być różnej postaci. Po pierwsze może to być dokumentacja, np. plan zarządzania konfiguracją, podręcznik dla personelu serwisującego czy dla administratora systemu, polityka bezpieczeństwa instytucji opracowującej (jej części dotyczącej środowiska rozwojowego TOE), lista konfiguracyjna, procedura instalacji systemu, procedura dostawy, dokumentacja testów, plan testów penetracyjnych i jeszcze wiele innych tego typu dokumentów – pod względem zawartości zawsze wynikających z odpowiednich wymagań typu SAR.

Materiałem dowodowym mogą być też udokumentowane wyniki niezależnych badań lub obserwacji prowadzonych przez oceniających, np. raport dotyczący analizy podatności TOE i jego środowiska rozwojowego, raport z niezależnego testowania TOE, raport z inspekcji środowiska rozwojowego TOE, czy też lista rankingowa przypadków ryzyka zidentyfikowanych w środowisku rozwojowym.

Ważnym rodzajem materiału dowodowego są również stwierdzone sposoby zachowania lub postępowania osób pełniących określone role w cyklu życia TOE, na przykład wynikające ze stosowania określonej procedury (akceptacji produktu lub systemu przed wysłaniem do klienta, itp.). Tego typu dowodem może być protokół, notatka czy tak zwane zapisy (ang. *records*), czyli różnego typu ślady operacji (dzienniki, logi – elektroniczne, bądź nie) odnotowywane przez system zarządzania.

Do materiału dowodowego zaliczane są również: zadanie zabezpieczeń (dla komponentów klasy ASE) oraz profil zabezpieczeń (dla komponentów klasy APE).

requirements (SAR) included in the declared EALn package (sometimes modified to EALn+). This documentation forms the so called evidences which are submitted for independent evaluation together with the TOE.

The evidences can have different forms. First, they can be documentation, e.g. a configuration management plan, manual for maintenance personnel or system administrator, security policy of the organization developing the product (the part referring to the TOE development environment), configuration list, system installation procedure, testing documentation, penetration tests plan, and many other documents of this kind which, in terms of their contents, always result from the proper security assurance requirements (SAR).

The evidences can also be documented results of independent examinations or observations carried out by the evaluators, e.g. a TOE (or TOE environment) vulnerability analysis report, independent TOE testing report, TOE development environment inspection report, ranking list of risks identified in this environment.

An important type of evidences are identified behaviours or actions of people who play certain roles in the TOE life cycle, for example the roles resulting from certain procedures (accepting the product or system before it is delivered to the client, etc.). This type of evidences includes: protocol, note, records – i.e. different traces of conducted operations (logs, including electronic ones) registered by the management system.

The evidences may also be: a security target (for ASE components) and protection profile (for APE components).

5. OCENA I CERTYFIKACJA PRODUKTÓW I SYSTEMÓW INFORMATYCZNYCH

Już w trakcie opracowywania produktu lub systemu informatycznego z myślą o jego certyfikacji jest nawiązywana współpraca z laboratorium oceniającym określony typ produktów, akredytowanym w ramach obowiązującego w danym kraju schematu certyfikacji. Taka współpraca, sprowadzająca się do prawie

5. EVALUATION AND CERTIFICATION OF IT PRODUCTS AND SYSTEMS

Already at an early of an IT product or system development, the developer starts co-operation with a certification body (evaluating certain types of products) accredited in a given country within the valid certification scheme. Such co-operation means that the IT product or system development process is ca-

współbieżnej oceny z konstruowaniem, jest bardzo korzystna, gdyż wykrywane przez oceniających problemy mogą być na bieżąco rozwiązywane. Można też przesłać do laboratorium gotowy już produkt, jednak wówczas wykrycie dowolnego problemu może powodować konieczność kosztownego przekonstruowania produktu.

Proces oceny produktu lub systemu informatycznego odbywa się z wykorzystaniem metodyki oceny [6].

Jak już wspomniano wcześniej, każdy komponent uzasadniający zaufanie (SAR) posiada trzy rodzaje elementów D, C i E. Metodyka oceny uszczegóławia elementy typu E podając, jak należy sprawdzać każdy z komponentów. Dostarcza ona zbioru zapytań dotyczących treści i postaci materiału dowodowego, pogrupowanych w tak zwane jednostki oceny (ang. *work unit*). Jednostki są poddawane ocenie z wykorzystaniem logiki trójwartościowej: *Pass* (werdykt pozytywny), *Fail* (werdykt negatywny) i *Inconclusive* (kwestia nierozstrzygalna). Każdy z werdyktów wymaga zwięzłego uzasadnienia. Najpierw przeprowadza się ocenę samego dokumentu ST (według komponentów klasy ASE), później samego TOE (według komponentów ADV, AGD, ALC, ATE i AVA). Można też oceniać same profile (według APE). Pozytywna ocena wszystkich jednostek oznacza ogólną ocenę pozytywną.

Pozytywny wynik oceny TOE i związanego z nim materiału dowodowego, wynik dodatkowo zweryfikowany przez jednostkę akredytującą dane laboratorium, pozwala na uzyskanie certyfikatu potwierdzającego, że produkt lub system informatyczny czyni zadość wymaganiom deklarowanego dla niego poziomu EAL.

Certyfikaty są publikowane na portalu Common Criteria [4]. Są tam umieszczane dokumenty zadań zabezpieczeń, profili zabezpieczeń oraz raporty z ich oceny wraz z dołączonymi certyfikatami. Stanowią one cenne źródło informacji dla:

- klientów, poszukujących produktów o odpowiedniej funkcjonalności i uzasadnionym zaufaniu,
- administratorów i użytkowników systemów, poszukujących wytycznych dotyczących ich bezpiecznego stosowania,
- menadżerów, decydujących o inwestycjach w technologie informatyczne,
- sponsorów, finansujących rozwój nowych produktów,
- konstruktorów i oceniających inne, podobne produkty.

rried out simultaneously with the evaluation process. This is very beneficial, as all drawbacks can be identified almost immediately by the evaluators. Of course it is possible to submit a ready product to the certification body, in this case, however, if a drawback or problem is found it might be necessary to redevelop the product, which is a costly process.

The IT product or system evaluation process is conducted with the use of the evaluation methodology [6].

As it was mentioned before, each SAR component has three types of elements: D, C and E. The evaluation methodology specifies E elements by giving information how each component should be checked. The methodology provides a set of questions referring to the contents and form of evidences, grouped in the so called work units. The work units are evaluated with the use of three-valued logic: pass, fail and inconclusive. Each of these verdicts needs short justification. First, the ST document is evaluated (according to the ASE class components), and then the TOE (according to ADV, AGD, ALC, ATE and AVA components). It is also possible to evaluate only profiles (according to APE). Positive evaluation (pass verdict) of all units means that the overall evaluation is positive too.

To obtain a certificate it is necessary to have a positive result of the TOE evaluation, including positive evaluation results of related evidences, as well as the verification of this result by an accreditation body which supervised a security evaluation lab. The certificate confirms that the IT product or system is compliant with the EAL declared for it.

The certificates are published on the Common Criteria portal. The portal also features security target and protection profile documents, as well as evaluation reports with accompanying certificates. These all are a valuable source of information for:

- clients who are looking for products with certain functionalities and assurance levels,
- system administrators and users who are looking for guidance how to use these systems in a secure way,
- managers who decide about investments in IT,
- sponsors who finance the development of new products,
- developers and evaluators of similar products.

Do tej pory oceniono około tysiąc produktów lub systemów informatycznych, głównie w zakresie środkowej części skali EAL. Są one bardzo różnorodne. Najwięcej jest typowych produktów informatycznych – kojarzonych z bezpieczeństwem (np. system zaporowy – firewall) lub też nie kojarzonych (np. system zarządzania bazą danych).

W ostatnim okresie pojawiają się nowe obszary zastosowań dotyczące na przykład systemów wbudowanych oraz czujników inteligentnych, na przykład czujników ruchu do tachografów cyfrowych. W tym sensie rysują się również możliwości wykorzystania standardu do rozwoju zaawansowanych urządzeń elektroniki i automatyki górniczej, których zabezpieczenia przed zagrożeniami zewnętrznymi również powinny cechować się odpowiednią wiarygodnością.

6. PODSUMOWANIE

Motywacją do opracowania niniejszego artykułu była chęć zainteresowania szerszego grona specjalistów – informatyków, elektroników oraz użytkowników wytwarzanych przez nich produktów lub systemów, dość mało znaną w Polsce tematyką kreowania uzasadnionego zaufania. Artykuł przedstawia w zarysie zagadnienia dotyczące tworzenia podstaw zaufania do produktów lub systemów informatycznych w świetle standardu Common Criteria (ISO/IEC 15408). Według prezentowanej metodyki źródłem tego zaufania jest rygorystyczny proces konstruowania oraz niezależna ocena prowadzona w akredytowanym laboratorium. Metodyka ta przynosi szereg korzyści [1], [7]:

- wymusza staranne projektowanie, testowanie, implementowanie i dokumentowanie produktu lub systemu informatycznego, w tym stosowanie dobrych praktyk i zasad inżynierskich, co ma szczególne znaczenie w przypadku oprogramowania,
- zwiększa zaufanie do produktów lub systemów informatycznych, zwłaszcza po ocenie prowadzonej w trakcie tworzenia produktu lub systemu,
- zmniejsza ryzyko stosowania technologii informatycznych do realizacji zadań biznesowych w różnych obszarach zastosowań,
- ułatwia użytkownikom wybór produktów lub systemów do ich specyficznych zastosowań i posiadających przy tym odpowiedni poziom uzasadnionego zaufania,

So far more than one thousand IT products or systems have been evaluated, most of them in the middle part of the EAL scale. These products and systems are quite varied. The majority are typical IT products associated with security (e.g. firewalls) or not (e.g. database management systems).

Recently, it has been possible to observe new application domains, for example those related to embedded systems or intelligent sensors, such as movement sensors for digital tachographs. Here there are also possibilities to use the standard in the development of advanced devices for mining electronics and automation. These devices should have reliable protection against external threats.

6. CONCLUSIONS

The motivation to prepare this paper was to popularize the issue of assurance development, still not much recognized in Poland, among experts, i.e. IT engineers and electronics engineers, and among the users of their products or systems. The paper is an overview of how to create assurance for IT products or systems with respect to the Common Criteria standard (ISO/IEC 15408). According to the presented methodology, the source of this assurance is a rigorous development process and independent evaluation carried out in an accredited laboratory. The methodology brings certain benefits [1], [7]:

- it enforces thorough development, testing, implementation, and documentation of an IT product or system, including the use of best practices and engineering principles, which is especially important in software development processes,
- it increases confidence to IT products or systems, particularly if their evaluation has been carried out during the product or system development,
- it reduces the risk of IT applications used to fulfill business tasks in different application areas,
- it makes it easier for the users to select a suitable product or system with an appropriate evaluation assurance level,

- ułatwia wejście z tymi wyrobami na obce rynki – certyfikaty posiadają międzynarodowy zasięg.

Przeciwnicy metodyki zarzucają jej złożoność, duży koszt procesów konstruowania i oceny produktów, jednak nie wydaje się by istniała dla niej jakaś alternatywa. Na pewno w dziedzinie bezpieczeństwa nie może być nią lansowana przez tych przeciwników tak zwana „droga na skróty".

Mimo, że metodyka się sprawdziła, to jednak jest ciągle doskonalona, by zmniejszyć koszt i czas realizacji projektów oraz poprawić ich dokładność. W nurt tych działań wpisują się również prace autora dotyczące formalizacji procesów konstruowania przez wykorzystanie modeli zapisanych w językach UML (*Unified Modelling Language*), OCL (*Object Constraints Language*) [8-13] oraz modeli bazujących na ontologiach [14]. Prace te mają na celu zwiększenie precyzji modeli i obniżenie kosztów projektowania, dzięki zastosowaniu komputerowego wspomagania.

Współpracę międzynarodową dotyczącą wydawania i wzajemnego uznawania certyfikatów Common Criteria, reguluje porozumienie CCRA (*Common Criteria Recognition Arrangement*), podpisane przez ponad 20 krajów. Wśród nich są kraje wiodące, które w pełni wdrożyły standard (wdrożyły swoje schematy certyfikacji, mają po kilka akredytowanych laboratoriów oceny, prowadzą oceny) i mają status „*Certificate Authorizing*". Pozostałe kraje posiadają status „*Certificate Consuming*", więc tylko honorują certyfikaty i są w trakcie przygotowań do pełnego wdrożenia. Nasz kraj niestety nie należy do żadnej z tych grup.

- it makes it easier for such products or systems to enter foreign markets due to international recognition of CC certificates.

The opponents of the CC methodology claim that it is complex and that the cost of IT products development and evaluation is high. Still, there seem to be no alternative to this methodology now. Certainly, the so called "shortcut" advertized by the opponents cannot be the one.

Though the methodology has proved to be successful, it is still being improved in order to reduce the cost and time of projects and to make them more precise. The author's works on the formalization of UML (*Unified Modelling Language*) models, OCL (*Object Constraints Language*) models [8-13] and ontology-based models [14] correspond to these activities. The works aim at improving the precision of models and reducing development costs thanks to the application of computer-aided tools.

International co-operation in the realm of issuing and mutual recognition of Common Criteria certificates is regulated in the Common Criteria Recognition Agreement (CCRA) signed by over 20 countries. The participants of CCRA are countries which have already implemented the standard (implemented their own evaluation and certification/validation schemes, have several accreditation laboratories, carry out evaluation processes) – these have the status of Certificate Authorizing Participants. The remaining countries are Certificate Consuming Participants, i.e. they only recognize the issued certificates and are in the process of full implementation of their own schemes. Unfortunately, Poland does not belong to any of these groups.

Literatura

1. ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security – Introduction and general model (Common Criteria Part 1).
2. ISO/IEC 15408-2, Information technology – Security techniques – Evaluation criteria for IT security – Security functional requirements (Common Criteria Part 2).
3. ISO/IEC 15408-3, Information technology – Security techniques – Evaluation criteria for IT security – Security assurance requirements (Common Criteria Part 3).
4. Common Criteria portal: http://www.commoncriteriaportal.org/
5. ISO/IEC TR 15446 Guide for the production of protection profiles and security targets.
6. Common Evaluation Methodology for Information Technology Security.
7. *Białas A.*: Konstruowanie zabezpieczeń produktów i systemów informatycznych posiadających mierzalny poziom uzasadnionego zaufania, Mechanizacja i Automatyzacja Górnictwa, Nr 1(455), styczeń 2009, Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG, Katowice, pp. 45-54.
8. *Białas A.*: Semiformal Common Criteria Compliant IT Security Development Framework. Studia Informatica vol. 29, Number 2B(77), Silesian University of Technology Press, Gliwice 2008.

References

1. ISO/IEC 15408-1, Information technology – Security techniques – Evaluation criteria for IT security – Introduction and general model (Common Criteria Part 1).
2. ISO/IEC 15408-2, Information technology – Security techniques – Evaluation criteria for IT security – Security functional requirements (Common Criteria Part 2).
3. ISO/IEC 15408-3, Information technology – Security techniques – Evaluation criteria for IT security – Security assurance requirements (Common Criteria Part 3).
4. Common Criteria portal: http://www.commoncriteriaportal.org/
5. ISO/IEC TR 15446 Guide for the production of protection profiles and security targets.
6. Common Evaluation Methodology for Information Technology Security.
7. *Białas A.*: Konstruowanie zabezpieczeń produktów i systemów informatycznych posiadających mierzalny poziom uzasadnionego zaufania, Mechanizacja i Automatyzacja Górnictwa, No 1(455), January 2009, Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG, Katowice, pp. 45-54.
8. *Białas A.*: Semiformal Common Criteria Compliant IT Security Development Framework. Studia Informatica vol. 29, Number 2B(77), Silesian University of Technology Press, Gliwice 2008.
9. *Białas A.*: IT security development – computer-aided tool supporting design and evaluation. W: Kowalik J., Górski J.,

Sachenko A. (eds.): Cyberspace Security and Defense. vol. 196, Springer Verlag, Heidelberg 2005, s. 3-23.
10. *Białas A.*: A semiformal approach to the security problem of the target of evaluation (TOE) modeling. W: Arabnia H., Aissi S. (Eds), Vert G., Williams P. (Assoc. Co Eds): Proc. of the 2006 Int. Conf. on Security and Management. CSREA Press, Las Vegas 2006, s. 19-25.
11. *Białas A.*: Semiformal Approach to the IT Security Development. W: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T.: Proceedings of the International Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007. IEEE Computer Society, Los Alamitos, Washington, Tokyo, s. 3-11.
12. *Białas A.*: Modeling the Security Objectives According to the Common Criteria Methodology. W: Aissi S., Arabnia H. (Editors), Daimi K., Gligoroski D., Markowsky G., Solo A.,M.,G. (Assoc. Co Eds), Proc. of the 2007 Int. Conf. on Security and Management. CSREA Press, Las Vegas 2007, s. 223-229.
13. *Białas A.*: Semiformal framework for ICT security development. The 8th International Common Criteria Conference (ICCC). Rome, 25-27 September 2007.
14. *Białas A.*: Ontology-based Approach to the Common Criteria Compliant IT Security Development, In: Arabnia H., Aissi S., Bedworth M (Eds.), Proceedings of the 2008 International Conference on Security and Management (The World Congress In Applied Computing – SAM'08: July, Las Vegas, USA), ISBN#1-60132-085-X, 2008, Publisher: CSREA Press, pp. 586-592.

Sachenko A. (eds.): Cyberspace Security and Defense. vol. 196, Springer Verlag, Heidelberg 2005, s. 3-23.
10. *Białas A.*: A semiformal approach to the security problem of the target of evaluation (TOE) modeling. W: Arabnia H., Aissi S. (Eds), Vert G., Williams P. (Assoc. Co Eds): Proc. of the 2006 Int. Conf. on Security and Management. CSREA Press, Las Vegas 2006, s. 19-25.
11. *Białas A.*: Semiformal Approach to the IT Security Development. W: Zamojski W., Mazurkiewicz J., Sugier J., Walkowiak T.: Proceedings of the International Conference on Dependability of Computer Systems DepCoS-RELCOMEX 2007. IEEE Computer Society, Los Alamitos, Washington, Tokyo, s. 3-11.
12. *Białas A.*: Modeling the Security Objectives According to the Common Criteria Methodology. W: Aissi S., Arabnia H. (Editors), Daimi K., Gligoroski D., Markowsky G., Solo A.,M.,G. (Assoc. Co Eds), Proc. of the 2007 Int. Conf. on Security and Management. CSREA Press, Las Vegas 2007, s. 223-229.
13. *Białas A.*: Semiformal framework for ICT security development. The 8th International Common Criteria Conference (ICCC). Rome, 25-27 September 2007.
14. *Białas A.*: Ontology-based Approach to the Common Criteria Compliant IT Security Development, In: Arabnia H., Aissi S., Bedworth M (Eds.), Proceedings of the 2008 International Conference on Security and Management (The World Congress In Applied Computing – SAM'08: July, Las Vegas, USA), ISBN#1-60132-085-X, 2008, Publisher: CSREA Press, pp. 586-592.

Recenzent: dr inż. Włodzimierz Boroń

9. *Białas A.*: IT security development – computer-aided tool supporting design and evaluation. W: Kowalik J., Górski J.,

ИНФОРМАТИЧЕСКИЕ ПРОДУКТЫ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ, А ТАКЖЕ СИСТЕМЫ С ЗАДАННЫМ УРОВНЕМ ОБЩИХ КРИТЕРИЕВ ОЦЕНКИ ЗАЩИЩЕННОСТИ ИНФОРМАЦИОННОЙ ТЕХНОЛОГИИ - (АНГЛ. COMMON CRITERIA FOR INFORMATION TECHNOLOGY SECURITY EVALUATION)

Статья описывает вопросы, связанные с конструированием и оценкой обеспечений, инсталлированных в произвольных продуктах либо в информатических системах. Выше перечисленные обеспечения относятся к полезным функциям и должны характеризоваться так называемыми общими критериями оценки защищенности информационных технологий, отождествляемыми обычно с достоверными. Представленная в статье методика Common Criteria, описанная в стандарте ISO/IEC 15408, является основной методикой создания общих критериев оценки защиты информационных технологий для информатического обеспечения. Методика охватывает три основных процесса. В процессе конструирования обеспечения на основании разного типа анализов безопасности, разрабатывается специальный документ называемый задачей обеспечений, образовывающий сбор требований безопасности - функциональных (как будут действовать обеспечения) и обосновывающих доверие (достоверность). Второй процесс касается конструирования продукта либо информатической системы, а также разработки его документации, составляющей расширение упомянутого задания обеспечения. Документация исполняет роль доказательственного материала а в третьем процессе – в процессе независимой оценки обеспечений, который должен довести к получению сертификата. Благодаря примененному строгому порядку конструирования, а также независимой и внимательной оценке, сертифицированные продукты признаваемы за более достоверные, благодаря чему более предрасположены к применениям, обремененным повышенным уровнем риска.