VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

Fakulta informačních technologií

KRITÉRIA HODNOCENÍ BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ

Habilitační práce

Brno 2003

Dr. Ing. Petr Hanáček

Obsah

Použité zkratky

ACL	Access Control List
ANSI	American National Standards Institute
BC	Bezpečnostní cíl
BFHP	Bezpečnostní funkcionalita HP
BPBF	Bezpečnostní politika bezpečnostní funkce
BPHP	Bezpečnostní politika HP
CA	Certifikační autorita
CAD	Computer Aided Design
CASE	Computer Aided Software Engineering
CBP	Celková bezpečnostní politika
CPS	Certifikační prováděcí směrnice
CC	Common Criteria
CP	Certifikační politika
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DoD	Department of Defense
EAL	Evaluation Assurance Level
FC	Federal Criteria for Information Technology Security
FIPS	Federal Information Procesing Standard
IEEE	Institute of Electrical and Electronics Engineers
HP	Hodnocený předmět
IS	Informační systém
ISCS	Informační systém pro poskytování certifikačních služeb
ISO	International Organization for Standardization
ISVS	Informační systém veřejné správy
IT	Informační technologie
ITSEC	Information Technology Security Evaluation Criteria
ITSEM	Information Technology Security Evaluation Manual
MLS	Multi Level Security
MSFR	Minimal Security Functional Requirements
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSI	Open Systems Interconnection
PCS	Poskytovatel certifikačních služeb
PKSPO	Plán pro zvládání krizových situací a plán obnovy
PO	Profil ochrany
SBP	Systémová bezpečnostní politika
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria
ZO	Zabezpečovaná oblast

1. Úvod

V průběhu několika posledních desetiletí začaly hrát informační technologie (IT) a jejich konkrétní realizace, informační systémy (IS), velmi důležitou, často rozhodující roli téměř ve všech oblastech lidské společnosti. Důsledkem tohoto prudkého rozvoje IT je i to, že důležitým aspektem IT se stává bezpečnost IT.

Vzhledem k širokému uplatnění IT i v netechnických oblastech společnosti nestačí pouze vytvořit bezpečný IS. Uživatel IS potřebuje *věřit*, že používaný IS je bezpečný. Uživatel také potřebuje *měřítko* pro porovnání bezpečnosti IS, který si hodlá pořídit. Z těchto uvedených důvodů se objevily snahy zavést nějaký standard, který by poskytoval uživatelům měřítko pro vyjádření stupně důvěry, kterou může uživatel vložit do IS a výrobcům IS prostředek pro vyjádření míry bezpečnosti nabízených IS. Tímto standardem jsou kritéria pro hodnocení bezpečnosti IS.

Předkládaná práce by měla poskytnout čtenáři přehled o nejrozšířenějších a nejpoužívanějších kritériích bezpečnosti IS, o jejich vývoji, významu a aplikacích. Protože autor aktivně působil a působí v oblasti zavádění těchto kritérií do praxe v naší republice, práce se soustřeďuje především na kritéria, která hrála nebo hrají nějakou roli v kontextu ČR.

Vlastní práce obsahuje nejprve několik kapitol, které jsou ve své podstatě komentovaným přehledem kritérií a jejich úkolem je v základech přiblížit metodiku, která je používána v prezentované vědní oblasti. Tyto kapitoly lze rozdělit do dvou skupin. První skupinu tvoří kapitoly, prezentující historický postup, kterým odborná komunita dospěla k současnému stavu v oboru. Druhá část rozšiřuje rozsah publikace o některé doplňující standardy a normy, které jsou třeba pro pokrytí potřeb hodnocení bezpečnosti typických systémů.

V práci je zvolen kompromis mezi podrobností a obecností. V textu jsou uvedeny základní pojmy a koncepty prezentovaných kritérií. Vzhledem k tomu, že jednotlivá kritéria vznikala postupně a byla i překládána z angličtiny postupně různými překladateli, nemají místy totožné názvosloví.

Přečtení těchto kapitol, doplněné případně o nahlédnutí do základní citované literatury, umožní čtenáři získat základní orientaci, postačující k snadnějšímu porozumění prezentovaných kritérií a základnímu přehledu v dané oblasti. Podrobné informace jsou dostupné s použitím odkazů na texty kritérií či speciální literaturu v odborných publikacích, uvedených v přehledu literatury.

Druhá část práce popisuje konkrétní nasazení některých prezentovaných postupů na konkrétním příkladu informačního systému pro poskytování certifikačních služeb. Tento příklad byl vybrán proto, že informační systémy poskytovatelů certifikačních služeb jsou první systémy v ČR, u kterých je požadováno hodnocení, hodnotitelnost nebo audit podle těchto kritérií. Je tedy i první oblastí, ve které jsou v ČR praktické zkušenosti s nasazením kritérií pro hodnocení bezpečnosti.

V této druhé části práce není popisováno nasazení kritérií na jeden konkrétní systém, jde spíše o syntézu postupů, z nichž některé byly aplikovány u různých konkrétních systémů a některé ještě v době psaní práce aplikovány nebyly, ale je vypracována jejich, alespoň rámcová, metodika. V některých případech jsou zvažovány i různé varianty toho, jak lze úspěšně dospět k výsledku, požadovanému pro tento informační systém.

Práce vznikla jako výsledek autorova více než desetiletého působení v oblasti bezpečnosti informačních systémů v ČR a to jak v oblasti pedagogické, v oblasti publikační, a také v oblasti spolupráce s některými orgány státní správy.

V některých částech práce autor rozsáhle cituje z některých svých významnějších publikací. Na rozdíl od citací z publikací jiných autorů, které jsou standardně označovány, nejsou citace z vlastních publikací autora označovány tam, kde by to narušovalo plynulost textu.

2. Bezpečnost informačních systémů

Bezpečnost informačních systémů je obor, který v současné době prochází bouřlivým rozvojem. Jeho rozvoj je dán především prudkou informatizací společnosti, jejímž důsledkem je stále větší závislost na informačních systémech, jejichž selhání může mít pro společnost závažné důsledky. S rozvojem informatizace se však také rozvíjejí negativní jevy, mezi než patří počítačová kriminalita, hackerství, crackerství, průmyslová počítačová špionáž a jiné nežádoucí činy. Proto dnes výstavba moderních, rozsáhlých a komplexních informačních systémů již není možná bez zabudování odpovídajících bezpečnostních mechanismů do těchto systémů. Stejně tak i provoz těchto systémů není možný bez odpovídajících bezpečnostních opatření. V poslední době se navíc objevují některé informační systémy, ve kterých náklady na bezpečnostní mechanismy tvoří podstatnou (někdy až převážnou) část celkových nákladů.

2.1 Historie bezpečnosti informačních systémů

Ačkoli elektronické počítače a tedy i elektronické informační systémy existují již přibližně půl století, je třeba říci, že obor "bezpečnost informačních systémů" zdaleka tak dlouhou historii nemá. Je sice pravdou, že údajně první číslicový počítač Colossus ([COL]) již v roce 1943 sloužil v anglickém dešifrovacím středisku v Bletchley Parku k luštění nepřátelských šifer, ale tento fakt lze těžko považovat za počátek bezpečnosti informačních systémů. Několik prvních desítek let své existence počítačové systémy existovaly bez toho, aby se nějakým způsobem zajišťovala jejich bezpečnost. Nebylo také proč. Tehdejší počítačové systémy zpravidla pracovaly v prostředí, kdy všichni uživatelé měli víceméně stejný zájem na správné funkci těchto systémů. To se však mělo změnit s postupujícím nasazením počítačů do běžných obchodních procesů.

V sedmdesátých letech se začínají poprvé objevovat první významnější počítačové bezpečnostní incidenty. Například v roce 1973 byla v New York City odhalena zpronevěra ve výši 1.2 milionu dolarů ([BW81]), kterou spáchal úředník spořitelny, který pomocí modifikace počítačového programu "odkrajoval" peníze z nově založených účtů s velkým zůstatkem. K jeho odhalení vedlo až jeho nápadné chování při sázení. Ve stejném roce byl odhalen akciový podvod velkého rozsahu ([PAR76]), při kterém pracovníci pojišťovny, nabízející životní pojistky, vytvořili asi 64000 "mrtvých duší", tedy neexistujících klientů, aby zvýšili cenu akcií pojišťovny. Pomocí počítače nejen že tyto klienty vytvořili, ale také pro ně vytvářeli legitimně vypadající účetní a auditní záznamy. V roce 1978 počítačový konzultant, pracující pro banku v Los Angeles, získal přístupové kódy, které mu umožnily převést nelegálně částku více než 10 milionů dolarů na svůj účet ve Švýcarsku ([BW81]). Přes to všechno je bezpečnost informačních systémů v této době pouze problémem některých odvětví státní správy, bank a podobných institucí.

Se začátkem osmdesátých let se začíná objevovat nový fenomén - neoprávněný přístup k počítačům pomocí telefonního připojení. V roce 1980 skupina teenagerů z Manhattanské Dalton School, později nazývaná "daltonský gang", využila školní počítač k útoku na kanadskou síť firemních i institucionálních počítačů a zničila některá cenná data. ([BW81]). Vzniká pojem klasického útočníka, který neoprávněně vzdáleně přistupuje k cizím počítačům - hackera. Filmovým symbolem této kategorie útočníků je film Válečné hry, jehož příběh je na tomto typu útoků založen. Po větší část osmdesátých let jsou tyto neoprávněné vzdálené přístupy k počítačům nejdominantnější hrozbou pro počítače. Je to umocněno mimo jiné tím,

že v USA se v té době silně rozmáhá vzdálená práce s počítačem přes modem, podporovaná v některých oblastech zanedbatelnými nebo žádnými poplatky za místní telefonní hovory a špatným zabezpečením počítačů. Z publikovaných seznamů nejvýznamnějších průniků však plyne, že hackeři způsobili přes velkou publicitu poměrně malé škody - nesrovnatelně menší, než například v té době vzniklé počítačové viry. Přestože jsou některé bezpečnostní incidenty tohoto období medializovány, bezpečnost informačních systémů je v této době stále jen problémem počítačových odborníků.

S rozvojem internetu v devadesátých letech dochází k tomu, že bezpečnost informačních systémů už není pouze záležitostí počítačových specialistů, ale začíná být důležitá i pro uživatele, kteří počítač používají pouze jako nástroj. Bezpečnost informačních systémů se v tomto období stává problémem i běžných uživatelů.

V posledních letech, s nástupem tzv. informační společnosti, dochází už k velmi silné závislosti lidské společnosti na informačních systémech. Informační systémy (a nyní už masově používané komunikační systémy) se stávají běžnou a těžko nahraditelnou součástí života. Na jejich činnosti jsou závislí lidé, kteří s počítači zdánlivě nemají nic společného a kteří třeba počítač ani nevlastní. Útoky na tyto informační systémy mohou nepříznivě ovlivnit i život těchto lidí. Bezpečnost informačních systémů se s mírnou nadsázkou stává i problémem běžných lidí.

2.2 Systematický přístup k bezpečnosti

Co je to vlastně bezpečnost informačního systému? Každý informační systém (IS) musí zajišťovat dodržování tří základních vlastností informace - důvěrnosti, integrity a přístupnosti. Co tyto pojmy znamenají:

- Důvěrnost (Confidentiality) je ochrana před neoprávněným zpřístupněním nebo odhalením informace.
- Integrita (Integrity) je ochrana před neoprávněnou modifikací nebo zničením informace.
- Dostupnost (Availability) je záruka, že informace bude na požádání dostupná oprávněným subjektům.

K těmto třem klasickým vlastnostem se brzy začala přidávat ještě vlastnost čtvrtá:

- Odpovědnost (Accountability) je schopnost informačního systému evidovat události, spojené s činností jednotlivých uživatelů.

Porušení kterékoli z výše uvedených zásad (tj. zpřístupnění informace neoprávněným subjektům, nesprávnost nebo nekompletnost informace, nepřístupnost informace pro oprávněné subjekty) znamená narušení bezpečnosti IS (bezpečnostní incident). U konkrétního IS je třeba definovat priority těchto zásad (v některých systémech může být primární důvěrnost i za cenu zhoršení přístupnosti, jindy je důležitá přístupnost bez ohledu na důvěrnost). Výše uvedené čtyři zásady se obvykle nazývají *bezpečnostní cíle*.

Splnění těchto bezpečnostní cílů je zajišťováno *bezpečnostními opatřeními*. Z hlediska svého typu se bezpečnostní opatření dělí na čtyři kategorie:

a) fyzická, jež se zabývají fyzickou ochranou jednotlivých částí IS

- kontrola přístupu do budov a místností, ochrana proti požáru, záplavě a teroristickému útoku, bezpečnostní vybavení nábytkem

b) personální, jež se podchycují spolehlivost a vlastnosti osob, jež jsou ve styku s IS

- programy bezpečnostního školení pro personál, dodržování bezpečnosti práce, zabránění zneužití zařízení, školení a vzdělávání personálu, havarijní plány (např. požární), právní otázky ochrany dat

c) procedurální, jež definují procedury, které musí být v rámci IS dodržovány

- definice osobní zodpovědnosti za bezpečnost, zálohování dat, péče o datová média, plánování mimořádných událostí, údržba programového a technického vybavení, bezpečnostní kontroly a inspekce, havarijní smlouvy a kontrakty, kontrola externích datových spojů, průběžná analýza rizika, vypracovávání zpráv o incidentech, autorizace přístupových práv k informacím, sledování přístupů k datům, klasifikace důvěrnosti a důležitosti dat, evidence vlastníků dat, dokumentace uložení dat na médiích

d) technická, která jsou implementována pomocí hardware a software

- sem patří všechny bezpečnostní funkce a mechanismy, které jsou implementovány v samotném informačním systému, jako je identifikace, autentizace, řízení přístupu atd.

Při popisu bezpečnostních opatření se převážně pracuje s popisem na úrovni tzv. *bezpečnostních funkcí*. Existuje mnoho různých klasifikací bezpečnostních funkcí, které jsou často vzájemně nekompatibilní. Jak uvidíme později, každá kritéria pro hodnocení bezpečnosti si definují svou vlastní sadu bezpečnostních funkcí, kterou pak používají. Proto se klasifikaci bezpečnostních funkcí budeme věnovat až při výkladu samotných kritérií.

3. Kritéria hodnocení bezpečnosti IS

Vzhledem k širokému uplatnění IT i v netechnických oblastech společnosti, nestačí pouze vytvořit bezpečný IS. Uživatel IS potřebuje *věřit*, že používaný IS je bezpečný. Uživatel tedy potřebuje *měřítko* pro porovnání bezpečností informačních systémů. Tímto měřítkem jsou standardy (kritéria) pro hodnocení bezpečnosti IS.

Kritéria jsou tedy určena pro tři typy uživatelů kritérií: pro uživatele IS, pro vývojáře IS (pod tímto názvem chápeme subjekty, které IS vyrábějí, kompletují a prodávají) a pro hodnotitele IS. Uživatelé a vývojáři informačních systémů tvoří nejčastější dvojici partnerů při jednání o bezpečnostních otázkách informačních systémů. Použití kritérií bezpečnosti může při jednání uživatele s vývojářem výrazně napomoci vzájemnému porozumění obou stran. Obě strany používají stejný jazyk, stejné názvosloví a i dokumenty, které používají, mají strukturu snadno srozumitelnou pro druhou stranu. I v případě, že obě strany nevedou přímý dialog, má použití kritérií bezpečnosti velký význam. V tom případě obě strany vypracovávají dokumenty, určené pro potenciálního nebo skutečného partnera. Tyto dokumenty mají obvykle formu specifikace bezpečnosti nebo bezpečnostního cíle. Uživatelé vytvářejí specifikace, které musí splňovat produkt (systém), který hodlají zakoupit. Prodejci vytvářejí specifikace produktu (systému), který nabízejí. V obou případech použití kritérií velmi usnadňuje tvorbu srozumitelné specifikace. Zvláštní skupinou uživatelů kritérií bezpečnosti jsou hodnotitelé. Jejich úkolem je ohodnotit konkrétní produkt (systém) vzhledem ke konkrétním kritériím bezpečnosti. Už z této definice je jasné, že jejich role je bez existence kritérií bezpečnosti nepředstavitelná.

Kritéria pro hodnocení bezpečnosti IS by tedy měla splňovat následující požadavky:

- Kritéria by měla poskytnout uživateli měřítko pro vyjádření stupně důvěry, kterou může uživatel vložit do IS, který chce použít pro zpracování důležitých informací.
- Kritéria by měla poskytnout výrobcům IS vodítko, které prvky bezpečnosti má zabudovat do vytvářeného IS, aby tento IS splňoval požadovaný stupeň bezpečnosti.
- Kritéria by měla poskytnout základ pro hodnocení stupně bezpečnosti IS certifikačním orgánem.

V následujících kapitolách se pokusíme poskytnout čtenáři přehled o nejrozšířenějších a nejpoužívanějších kritériích bezpečnosti IS.

3.1 Trusted Computer System Evaluation Criteria (TCSEC)

USA začaly s vývojem kritérií bezpečnosti IS v roce 1967, kdy byla sestavena pracovní skupina pod vedením ministerstva obrany (Department of Defense, DoD), která měla za úkol vypracovat pravidla bezpečnosti pro víceuživatelské počítačové systémy se vzdáleným přístupem. Výsledkem práce této skupiny byla zpráva 5200.28M, kterou DoD publikovalo v roce 1972. Tento dokument specifikoval bezpečnostní politiku, bezpečnostní požadavky a administrativní a technická bezpečnostní opatření v podmínkách DoD.

V roce 1977 byla započata na DoD systematická práce na vytváření bezpečnostních kritérií a byla založena pracovní skupina pod názvem DoD Computer Security Initiative. Ta byla transformována v roce 1981 ve výzkumné středisko DoD Computer Security Center. Toto

středisko v roce 1983 publikovalo patrně nejznámější standard pro bezpečnost IS, DoD 5200.28 STD ([TCSEC]), známý pod jménem TCSEC nebo oranžová kniha (Orange Book).

Publikace TCSEC je jednou ze série publikací DoD týkajících se bezpečností IS. Tato série je nazývána "Rainbow Series" a skládá se asi z 25 publikací. Nejznámější z této série jsou následující tři publikace:

- "*Orange Book*", neboli Trusted Computer Systems Evaluation Criteria (TCSEC, [TCSEC]), která definuje požadavky bezpečnosti pro počítačové informační systémy,
- "*Grey Book*", neboli Trusted Database Interpretation ([TG2191]), která definuje standardy bezpečnosti pro databázové aplikace,
- "*Raspbery Book*", neboli Trusted Network Interpretation, která definuje standardy bezpečnosti pro počítačové sítě.

Nejdůležitější z těchto publikací je publikace TCSEC, a proto se jí budeme věnovat trochu podrobněji. Tato publikace byla poprvé zveřejněna v roce 1983 a upravena v roce 1985. Stala se prvním obecně dostupným dokumentem, který popisuje obecné bezpečnostní požadavky, které lze aplikovat na konkrétní část informačního systému (např. na operační systém). Informační systémy jsou podle stupně své bezpečnosti rozděleny do čtyř *tříd bezpečnosti* A, B, C a D. Třída D znamená nejmenší míru bezpečnosti, třída A znamená míru největší. Stručně lze tyto čtyři třídy charakterizovat takto: Třída D obsahuje IS s minimálními nebo žádnými prvky bezpečnosti. Třída C obsahuje IS s volitelnou (nepovinnou) definicí přístupových práv (sem spadá většina současných IS). Třída B obsahuje IS s povinnou definicí přístupových práv a s klasifikací dat podle stupně ochrany dat. Konečně třída A obsahuje IS, jejichž prvky bezpečnosti splňují vše, co je požadováno ve třídě B a navíc je proveden formální důkaz správnosti těchto prvků.

Třídy bezpečnosti A, B a C se dělí dále na *podtřídy bezpečnosti*, které jsou číslovány (A1, B1, B2, B3, C1 a C2). Při klasifikaci IS se jména tříd A až C neužívají - užívá se vždy jméno podtřídy. V následujících odstavcích budou všechny podtřídy TCSEC popsány detailněji.

Třída D: **Minimální nebo žádná ochrana**

V této třídě nejsou na IS kladeny žádné požadavky z hlediska bezpečnosti. Tato třída je vyhrazena pro IS, které jsou hodnoceny z hlediska bezpečnosti, ale které nemohou být zařazeny do některé vyšší třídy.

Třída C1: **Volitelná bezpečnostní ochrana**

IS ve třídě C1 musí umožňovat pomocí nepovinného řízení přístupu volitelnou ochranu dat a volitelnou definici přístupových práv. Musí poskytovat možnost izolace prostředí jednotlivých uživatelů a jejich dat. Uživatel musí mít možnost chránit svá data před jinými uživateli. Systém musí nabízet ochranu dat před neúmyslným poškozením a před mírnějším úmyslným útokem. Pokud IS pracuje s klasifikovanými daty, předpokládá se, že všichni uživatelé pracují s daty stejného stupně utajení.

Třída C2: **Řízený systém přístupových práv**

Ve třídě C2 se požaduje všechno, co ve třídě C1. Volitelná definice přístupových práv musí umožňovat jemnější přidělení práv. Vyžaduje se jednoznačná identifikace a autentizace každého uživatele. Systém musí umožnit vytvářet auditní záznam událostí významných z hlediska bezpečnosti. Vyžaduje se rušení obsahu objektů při jejich opakovaném použití.

Třída B1: **Povinná bezpečnostní ochrana**

Systémy v této třídě musí splňovat všechny požadavky třídy C2. Musí existovat alespoň neformální definice bezpečnostní politiky IS. Systém musí zajišťovat povinnou definici přístupových práv pro všechny pojmenované objekty a subjekty. Data musí být klasifikována z hlediska bezpečnosti. Musí být rovněž klasifikovány všechny informace exportované ze systému.

Třída B2: **Strukturovaná ochrana**

Systémy v této třídě musí splňovat všechny požadavky třídy B1. Musí existovat formální definice bezpečnostní politiky IS. Povinná definice přístupových práv je rozšířena na všechny subjekty a objekty v systému. Musí být provedena analýza skrytých kanálů. IS musí být strukturován na části, které jsou kritické z hlediska bezpečnosti a na části, které kritické nejsou. Je zesílen autentizační mechanismus. Je zaveden pojem důvěryhodné zařízení. IS musí odolat všem běžným úmyslným útokům.

Třída B3: **Bezpečnostní domény**

V této třídě musí autorizaci prověřovat správce přístupu k objektu. Správce přístupu k objektu musí být odolný proti fyzickému útoku a musí být dostatečně malý, aby mohl být podroben analýze a testování. Je zajištěno jednoznačné určení odpovědnosti správců. Auditní mechanismus dovoluje on-line detekci nebezpečných stavů. Je zajištěno bezpečné zotavení systému po poruše nebo po útoku. Systém musí odolat i silnému úmyslnému útoku.

Třída A1: **Verifikovaný návrh**

Na systém v této třídě jsou kladeny stejné funkční požadavky jako na systém ve třídě B3. Třída A1 však požaduje, aby bylo formálně dokázáno, že jsou splněny funkční požadavky. Musí existovat formální model bezpečnostní politiky a návrh IS musí být prováděn pomocí formální specifikace shora dolů.

3.2 Další iniciativy v USA

Po zavedení TCSEC se ukázalo, že tato kritéria sice jsou velmi hodnotným výchozím bodem pro zavádění standardizace bezpečnosti IS, ale že nejsou dostatečná pro komerční aplikace. Bylo to způsobeno hlavně místem jejich vzniku ve vojenském prostředí. Proto se některé komerční společnosti rozhodly vytvořit svá vlastní kritéria bezpečnosti IS. Nejúspěšnější v tomto směru byla firma Bellcore a firma American Express Travel Related Services (TRS).

Firma Bellcore vytvořila dokument s názvem *Bellcore Standard Operating Environment Security Requirements*. Tento dokument nebyl koncipován příliš obecně a vycházel z TCSEC, z obecně používaných zásad bezpečnosti IS a ze zkušeností bezpečnostního oddělení firmy Bellcore.

Firma TRS vytvořila jako svůj bezpečnostní standard dokument pod názvem *C2-Plus*. Při jeho návrhu došla k závěru, že standard TCSEC sice splňuje většinu požadavků potřebných v komerčním sektoru, ale pro jeho praktické prosazení je třeba provést několik úprav. Za hlavní nedostatek považovala to, že třída bezpečnosti C2 (jako třída, jejíž realizace byla momentálním cílem) neobsahuje některé rysy, které jsou buďto zavedeny až ve třídách vyšších nebo nejsou v dokumentu TCSEC zachyceny vůbec. Dokument C2-Plus se vlastně zabýval pouze definicí rozšířených, komerčně zaměřených požadavků pro třídu C2. Dokument C2-Plus byl pouze

firemním standardem firmy TRS, ale později se stal základem mezinárodního standardu *Commercial International Security Requirements* (CISR), který vytvořila organizace International Information Integrity Institute (I-4). Tento dokument byl publikován v roce 1992.

Minimum Security Functionality Requirements (MSFR)

Dokument MSFR ([MSFR]) byl vytvořen v lednu 1992 pracovní skupinou, která se zabývala také přípravou vládního dokumentu FC (viz dále). Při vytváření dokumentu se předpokládalo, že hlavní myšlenky MSFR budou zabudovány po nezbytných úpravách i do dokumentu FC. Cílem zveřejnění těchto myšlenek v dokumentu MSFR bylo jednak umožnit dřívější používání těchto kritérií (vydání dokumentu FC bylo tehdy v nedohlednu) a jednak seznámit veřejnost se směrem vývoje připravovaného dokumentu FC a získat připomínky potenciálních uživatelů dokumentu FC.

Cílem pracovní skupiny MSFR bylo vytvořit třídu požadavků, která by nahradila třídu bezpečnosti C2 TCSEC. Tato nová třída je orientována směrem k IS, které nezpracovávají klasifikované druhy informace (na rozdíl od vojenských IS, které zpracovávají informace přísně klasifikované podle stupně utajení) ve státních a komerčních organizacích. Třída se také orientuje více na specifika IS postavených na bázi víceuživatelských operačních systémů. MSFR je při srovnání s TCSEC C2 modernizován, poskytuje podrobnější a detailnější popis požadovaných bezpečnostních opatření a také podrobnější instrukce pro tvůrce IS. Je zajištěna i kompatibilita s jinými standardy. Informační systém, který vyhovuje MSFR, také splňuje třídu C2 kritérií TCSEC a třídu E2 evropských kritérií ITSEC (viz kapitola o ITSEC).

Federal Criteria for Information Technology Security (FC)

Kritéria bezpečnosti IS pod názvem FC ([FC]) jsou společným dílem organizací National Institute of Standards and Technology (NIST) a National Security Agency (NSA). Motivace pro vznik dokumentu FC byla dvojí. Prvním důvodem je potřeba nahradit dokument TCSEC, který už přestával vyhovovat. Druhým důvodem byla je snaha harmonizovat kritéria bezpečnosti IS v mezinárodním měřítku.

Dokument FC se skládá ze dvou částí. První část definuje pojmy a stupnice kritérií pro jednotlivé funkce a cíle bezpečnosti IS. Jako příklad použití definovaných pojmů je uvedena definice sedmi tříd bezpečnosti T1 až T7 a korespondence těchto tříd s třídami TCSEC. Díl druhý obsahuje všeobecně přijaté bezpečnostní profily, které by měly uživateli pomoci nalézt produkt, který vyhovuje jeho bezpečnostním požadavkům.

3.3 Evropská kritéria bezpečnosti IS

Z evropských standardů pro hodnocení bezpečnosti IS stojí za zmínku kritéria britská a německá. Britská kritéria bezpečnosti IS vyšla v roce 1989 pod názvem UK Systems Security Confidence Levels. Tato kritéria definují šest hodnotících tříd L1 až L6. Mimo to kritéria definují ještě tzv. *požadavkový jazyk*, pomocí něhož lze popsat bezpečnostní vlastnosti produktu pomocí poloformální notace. Tento požadavkový jazyk byl pak převzat evropskými kritérii ITSEC.

Německá kritéria bezpečnosti IS vyšla rovněž v roce 1989 pod názvem IT-Sicherheitskriterien: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik ([ITSICH]). Kritéria definují osm tříd kvality Q0 až Q7 a deset tříd funkčnosti F1 až F10. Hodnocený produkt je pak označen dvojicí {Třída funkčnosti, Třída kvality}. Mezi IT-Sicherheitskriterien

a TCSEC existuje jednosměrná korespondence, to znamená, že každou třídu TCSEC je možno vyjádřit pomocí IT-Sicherheitskriterien ale nikoli naopak.

Britská a německá kritéria hodnocení bezpečnosti IS (spolu s kritérii francouzskými a nizozemskými) byla základem pro vytvoření společných evropských kritérií ITSEC. Těmto kritériím je věnován následující text.

3.4 Kritéria bezpečnosti ITSEC

Kritéria pro hodnocení bezpečnosti IT ITSEC (Information Technology Security Evaluation Criteria, [ITSEC], [ITSECcz]) byla vytvořena v roce 1990. Byla vytvořena jako harmonizovaná verze národních kritérií přijatých ve Francii, Německu, Velké Británii a Nizozemí. Kritéria byla předložena v září 1990 v Bruselu k připomínkám a diskusi, které se zúčastnily i USA. Po úpravách byla vydána Úřadem pro oficiální publikace Evropského společenství v červnu 1991 jako prozatímní materiál k dvouletému ověření. Jako doporučení byla schválena v dubnu 1995.

V září 1993 byl Úřadem pro oficiální publikace Evropského společenství vydán prováděcí manuál ke kritériím ITSEC pod názvem Information Technology Security Evaluation Manual, zkráceně ITSEM ([ITSEM], [ITSEMcz]). ITSEM je vypracován jako nadstavba nad kritérii ITSEC verze 1.2. Jeho účelem je popsat, jak má být hodnocen hodnocený předmět v souladu s požadavky kritérií ITSEC. ITSEM obsahuje harmonizovanou metodologii pro hodnocení bezpečnosti IS (zatímco ITSEC obsahuje harmonizovaná kritéria pro hodnocení bezpečnosti IS) a tím vytváří komplementární dokument k dokumentu ITSEC.

V terminologii ITSEC je produkt nebo systém, který bude hodnocen, nazýván *hodnocený předmět* (HP). Strana, která nabízí předmět hodnocení, je nazývána *sponzor*. Sponzor musí předložit k posouzení produkt nebo systém spolu se zdokumentovanou specifikací svého bezpečnostního cíle, potenciálních hrozeb a příslušných protiopatření a mechanismů. Hodnotitel má povinnost otestovat hodnocený předmět a porovnat výsledky s bezpečnostním cílem, specifikovaným sponzorem. Podle výsledků hodnocení pak hodnotitel vydá certifikát.

ITSEC specifikuje sedm tříd míry záruky E0 až E6 a v příloze definuje dalších deset tříd funkčnosti F. Třídy míry záruky vycházejí ze čtyř základních skupin kritérií: proces vývoje IS, prostředí vývoje IS, provozní dokumentace IS a provozní prostředí IS. Pět tříd funkčnosti F-C1, F-C2, F-B1, F-B2 a F-B3 odpovídají stejnojmenným třídám kritérií TCSEC. Zbylých pět tříd funkčnosti je orientováno aplikačně. Na rozdíl od TCSEC, která vznikala pro vojenské prostředí a orientovala se zejména na důvěrnost informace, je TCSEC koncipován mnohem obecněji a pokrývá částečně i požadavky integrity a dostupnosti informace. Oproti TCSEC definuje ITSEC navíc způsob dokumentace hodnoceného předmětu, způsob definování bezpečnostního cíle a způsob provádění hodnocení.

3.4.1 Hlavní části kritérií ITSEC

Z hlediska běžného uživatele poskytují kritéria ITSEC tři nejdůležitější komponenty:

- požadavky na míru záruky
- požadavky na funkčnost
- požadavky na definici produktu/systému

V dalších odstavcích se budeme těmito komponentami zabývat podrobněji.

3.4.2 Požadavky na míru záruky a požadavky na funkčnost

V kritériích ITSEC jsou požadavky na míru záruky a na funkčnost specifikovány odděleně. Oddělená existence těchto dvou skupin požadavků vlastně definuje charakter kritérií ITSEC - jde o kritéria, která jsou "dvojrozměrná", to znamená, že u každého produktu lze odděleně hodnotit funkčnost a míru záruky. Tento rys kritérií ITSEC je pravděpodobně nejvýznamnější výhodou těchto kritérií oproti kritériím "jednorozměrným", jako jsou například kritéria TCSEC. V kritériích TCSEC je definována pouze jedna lineární hierarchie tříd, která v sobě zahrnuje jak požadavky funkčnosti, tak i požadavky na míru záruky. Pokud si uživatel zvolí určitou třídu podle požadavků na funkčnost, musí se smířit i s požadavky na míru záruky definovanými v této třídě, přestože tyto požadavky mohou být v některých případech neadekvátní požadavkům uživatele. Při použití kritérií ITSEC si může uživatel zvolit nezávisle téměř libovolnou kombinaci požadavků na funkčnost a míru záruky.

Definice kritérií míry záruky tvoří rozsahem největší část kritérií ITSEC. V této části je definováno sedm tříd míry záruky E0 až E6. Přestože názvy těchto tříd neodpovídají ničemu, co čtenář zná z kritérií TCSEC, existuje mezi třídami TCSEC a ITSEC přímá relace. Tato relace je uvedena v následující tabulce (podobnou tabulku čtenář nalezne i v [ITSEC], odstavec 1.39).

ITSEC	TCSEC
E0	D
E1	C1
E2	C2
E3	B1
E4	B2
E5	B3
E6	A1

Tabulka 3.1 Vztah tříd míry záruky ITSEC a tříd TCSEC

Zatímco pro požadavky na míru záruky je v kritériích ITSEC definováno sedm tříd E0 až E6 a nepředpokládá se, že by uživatelé kritérií definice těchto tříd měnili nebo si definovali své vlastní třídy, u požadavků na funkčnost je tomu jinak. U těchto požadavků kritéria ITSEC nepředepisují žádnou apriori danou množinu tříd funkčnosti. Místo toho pouze definují zásady, jak takovou třídu funkčnosti vytvořit. Pro usnadnění práce uživatelům kritérií a pro kompatibilitu s jinými kritérii jsou v příloze kritérií ITSEC uvedeny příklady tříd funkčnosti. Pět z těchto tříd funkčnosti (třídy F-C1, F-C2, F-B1, F-B2 a F-B3) je hierarchických a přímo odpovídá požadavkům funkčnosti stejnojmenných tříd kritérií TCSEC. To umožňuje uživateli, který požaduje kompatibilitu s kritérii TCSEC, zvolit třídy ohodnocení ekvivalentní třídám kritérií TCSEC.

Zbylých pět tříd funkčnosti (F-IN, F-AV, F-DI, F-DC a F-DX) nemá hierarchickou strukturu. Těmito třídami funkčnosti jsou třídy se zvýšenými bezpečnostními požadavky v některé oblasti bezpečnosti - například F-IN je třída se zvýšenými požadavky v oblasti integrity, F-AV je třída se zvýšenými požadavky v oblasti dostupnosti atd.

Výše uvedené třídy funkčnosti jsou, na rozdíl od tříd míry záruky, pouze příklady. Nejsou závazné a mají sloužit pro usnadnění práce uživatelům kritérií ITSEC. Proto má uživatel kritérií několik možností, jak kategorizovat funkčnost produktu nebo systému.

První možností je, že uživatel přímo použije některou ze tříd funkčnosti, uvedenou v kritériích ITSEC. V tomto případě si zpravidla vybere některou ze tříd, které jsou hierarchické a odpovídají třídám kritérií TCSEC.

Druhou možností je, že uživatel kritérií použije vhodné kombinace některých ze tříd funkčnosti, uvedených v kritériích ITSEC. Tato možnost dává uživateli kritérií větší možnosti a dovoluje mu vytvořit třídu funkčnosti, která lépe odpovídá jeho požadavkům.

Třetí možností je, že uživatel kritérií použije některou, již vytvořenou třídu funkčnosti, která není součástí kritérií ITSEC, ale je vytvořena v souladu s těmito kritérii a nejlépe vyhovuje požadavkům uživatele. Příkladem takovéto třídy funkčnosti je třída funkčních požadavků pro víceuživatelské operační systémy. Tato třída je vytvořena v souladu s požadavky kritérií ITSEC a je vhodná pro hodnocení bezpečnosti moderních operačních systémů.

Konečně poslední, čtvrtou, možností je případ, kdy si uživatel kritérií vytvoří sám vlastní třídu funkčnosti, která je v souladu s požadavky kritérií ITSEC. Tento případ nastane zejména v okamžiku, kdy je hodnocený předmět natolik specifický, že jsou všechny výše uvedené cesty neschůdné. Vzhledem k pracnosti tohoto způsobu stojí však vždy za úvahu, zda skutečně nelze využít některý ze tří výše uvedených případů.

3.4.3 Generická záhlaví požadavků na funkčnost

V případě, že se uživatel kritérií rozhodne vytvořit si vlastní třídu funkčnosti, doporučuje se, aby použil systém generických záhlaví, která jsou definována v kritériích ITSEC. Jedná se o tato generická záhlaví:

Identifikace a autentizace

Toto záhlaví musí pokrýt všechny funkce, které umožní přidávání nových a rušení starých identifikací uživatelů. Podobně sem musí patřit všechny funkce, které generují, mění nebo umožňují autorizovaným uživatelům prohlédnout si (zkontrolovat) autentizační informace požadované k ověřování identity uživatelů. Zahrnuje rovněž funkce, které zajišťují integritu autentizačních informací nebo brání před neautorizovaným užitím této informace. Pokrývá také funkce, které omezují příležitost k opakovaným pokusům o zadání falešné identity.

Řízení přístupu

Toto záhlaví musí pokrýt všechny funkce, určené k vytváření seznamů nebo pravidel, kterými se řídí přístupová práva pro různé typy přístupů. Patří sem funkce dočasně omezující přístup k objektům, které jsou současně přístupné několika uživatelům nebo procesům, přičemž musí být zachována konzistence a neporušenost těchto objektů. Patří sem také funkce, které zajistí vytvoření implicitních přístupových seznamů nebo přístupových pravidel k objektům. Musí obsahovat všechny funkce, které řídí šíření přístupových práv k objektům. Musí zahrnovat

rovněž funkce řídící dedukci informací, které vzniknou agregací dat z jinak legitimních přístupů.

Účtovatelnost

Toto záhlaví musí pokrýt všechny funkce, které se vztahují ke shromažďování informací o činnostech a událostech relevantních z hlediska bezpečnosti, k ochraně a analýze takových informací. Některé funkce mohou splňovat požadavky, které mají vztah k účtování i k auditu a spadají tak pod obě záhlaví. Takové funkce mohou být zahrnuty pod jedno záhlaví a přitom musí být odkazovány i pod záhlavím druhým.

Audit

Toto záhlaví musí obsahovat funkce určené k manuálnímu nebo automatickému zkoumání protokolu o relevantních událostech v IS z hlediska bezpečnosti, ke shromažďování, ochraně a analýze takových informací. Prováděné analýzy mohou také zahrnovat detekci potenciálních hrozeb bezpečnosti ještě předtím, než dojde k útoku. Některé funkce mohou splňovat požadavky na účtovatelnost i audit, takže mají vztah k oběma záhlavím. Takové funkce mohou být uváděny pod jedním záhlavím a zároveň musí být odkazovány i pod druhým záhlavím.

Opakované užití

Toto záhlaví musí pokrýt všechny funkce určené k inicializaci nebo mazání nepřidělených nebo opakovaně přidělených datových objektů. Obsahuje rovněž funkce určené k inicializaci nebo mazání opakovaně použitelných médií, jako jsou magnetické pásky a disky, nebo mazání výstupních zařízení, jako jsou obrazovky displejů, které nejsou právě užívány.

Přesnost

Toto záhlaví musí pokrýt všechny funkce, které určují, zavádějí a udržují přesnost vztahů mezi odpovídajícími daty. Obsahuje rovněž funkce, které zajišťují, že u dat přenášených mezi procesy, uživateli a objekty je možno detekovat nebo předcházet ztrátám nebo modifikacím a že není možno změnit předpokládaný nebo reálný zdroj a místo určení při přenosu dat.

Spolehlivost a dostupnost služeb

Toto záhlaví musí pokrýt všechny funkce, které zajišťují, aby zdroje byly přístupné a využitelné na základě požadavků autorizované entity (uživatele, procesu pod jeho jménem) a zabraňují interferencím mezi časově kritickými operacemi, případně tyto interference omezují.

Toto záhlaví musí zahrnovat funkce určené k detekci chyb a zotavení po chybě s cílem omezit vliv chyb na činnost produktu nebo systému, a minimalizovat tak přerušení nebo ztrátu služeb. Patří sem také všechny plánované funkce, které zajišťují, aby produkt nebo systém reagoval na externí události a produkoval výstupy v zadaných časových limitech.

Výměna dat

Toto záhlaví musí pokrýt všechny funkce, které zajišťují bezpečnost dat při přenosu komunikačními kanály. Doporučuje se, aby tyto funkce byly rozděleny podle záhlaví,

vybraných z bezpečnostních architektur OSI (Open Systems Interconnection, [ISO7498]): autentizace, řízení přístupu, důvěrnost dat, integrita dat, nepopiratelnost.

Použití generických záhlaví je v kritériích ITSEC pouze doporučováno, není striktně vyžadováno, nelze však než doporučit čtenáři, aby tato záhlaví používal.

3.4.4 Proces hodnocení podle kritérií ITSEC

V následujících odstavcích stručně popíšeme proces hodnocení bezpečnosti systému nebo produktu IT podle metodiky kritérií ITSEC, tak jak je tento postup navržen v publikaci [ITSEM].

Procesu hodnocení se účastní čtyři subjekty: sponzor hodnocení, vývojář, hodnotící organizace a certifikační orgán.

Sponzor hodnocení je obvykle prodejce (v případě produktu) nebo uživatel či dodavatel (v případě systému), který si přeje demonstrovat, že hodnocený předmět splňuje specifikaci bezpečnosti. Sponzor iniciuje hodnocení produktu hodnotící organizací. Zajistí vypracování specifikace bezpečnosti a uzavírá kontrakt s hodnotící organizací. Pokud hodnocení dopadne úspěšně, sponzor obdrží od certifikačního orgánu certifikát bezpečnosti.

Názvem *vývojář* se obvykle označuje organizace, která vyrábí hodnocený předmět. Pokud vývojář není zároveň i sponzorem, musí spolupracovat se sponzorem hodnocení a musí spolupracovat i s hodnotící organizací.

Úkolem *hodnotící organizace* je provádět nezávislé hodnocení hodnoceného předmětu. Cílem je nalézt slabiny hodnoceného předmětu a určit, v jakém rozsahu jsou splněny požadavky, uvedené ve specifikaci bezpečnosti. Hodnocení musí být provedeno v souladu s dokumenty ITSEC a ITSEM a v souladu s národními normami země, kde se hodnocení provádí. Hodnotící organizace vypracovává zprávu o hodnocení, kterou předá certifikačnímu orgánu a sponzorovi.

Certifikační orgán je státní organizace, která jako jediná má oprávnění vydávat certifikát bezpečnosti informačního systému. Tento certifikát stvrzuje, že úroveň bezpečnosti hodnoceného předmětu odpovídá požadavkům, uvedeným ve specifikaci bezpečnosti a že hodnocený předmět dosáhl některé třídy míry zaručitelnosti bezpečnosti podle kritérií ITSEC. Certifikační orgán má dva úkoly:

- Vytváří hodnotící organizaci podmínky pro nestranné a objektivní hodnocení a kontroluje dodržení nestrannosti, objektivity a konzistence hodnocení.
- Vydává nestranné potvrzení (certifikát) bezpečnosti.

Hodnocení produktu (systému) se provádí ve třech fázích:

1. *Přípravná fáze*. V této fázi sponzor kontaktuje všechny účastníky hodnocení, uzavře s nimi kontrakty a zajistí vypracování specifikace bezpečnosti, kterou dá všem účastníkům. Hodnotící organizace provede odhad předpokládané úspěšnosti hodnocení a v kladném případě se ujme hodnocení.
2. *Vlastní hodnocení*. Během této fáze hodnotící organizace provádí vlastní hodnocení hodnoceného předmětu. Je vytvořen seznam slabých míst hodnoceného předmětu. Případné problémy jsou řešeny podle jejich charakteru buď v součinnosti s certifikačním orgánem, nebo v součinnosti se sponzorem hodnocení a s vývojářem.

Během hodnocení je hodnotící organizací vypracována zpráva o hodnocení. Tato zpráva je pak předána sponzorovi hodnocení a certifikačnímu orgánu.

3. *Závěrečná fáze*. V této fázi certifikační orgán analyzuje výsledky hodnocení, uvedené ve zprávě o hodnocení a určí, zda byly splněny požadavky, uvedené ve specifikaci bezpečnosti. V kladném případě udělí hodnocenému předmětu certifikát a předá jej sponzorovi.

3.4.5 Kritické zhodnocení kritérií ITSEC

Je nutno konstatovat, že obsah dokumentu ITSEC neodpovídá zcela jeho názvu. Prvním důvodem je, že nejde zcela o "kritéria". O kritéria jde pouze v části, zabývající se mírou zaručitelnosti bezpečnosti, kde jsou definovány třídy míry zaručitelnosti E0 až E6. V části, zabývající se bezpečnostní funkčností, však jde spíše o návod, jak vypracovat kritéria, neboli jedná se spíše o "generická kritéria".

Dokument ITSEC nezahrnuje informační systémy s distribuovanou správou, to jest vzájemně propojené informační systémy s několika správci, jejichž zájmy mohou být rozdílné. Přestože jde o poměrně obtížnou a dosud nepříliš zpracovanou problematiku, bylo by vhodné, aby se jí dokument zabýval. Této problematiky se v dokumentu dotýká pouze odkaz na bezpečnostní mechanismy nepopiratelnosti, což však zdaleka nepostačuje. Na základě výše uvedených důvodů by tedy bylo vhodnější, kdyby se dokument ITSEC nazýval spíše "Generická kritéria pro hodnocení bezpečnosti hierarchicky spravovaných systémů IT".

Kritika definice integrity

Integrita je v materiálu ITSEC definována jako "prevence proti neautorizované modifikaci informace". Tato klasická definice je sice uváděna i v jiných materiálech, ale není právě šťastná. Její nevhodnost se ukazuje např. v prostředí distribuovaných informačních systémů. V těchto systémech při přenosu dat veřejnou datovou sítí zpravidla nelze zabránit neautorizované modifikaci informace bez použití velmi nákladných (a zpravidla prakticky nerealizovatelných) fyzických bezpečnostních opatření. Neautorizovanou modifikaci dat lze však detekovat (např. kryptografickými prostředky) a na základě této detekce lze přenos dat opakovat. Pokud při každém pokusu o přenos dat dojde k neautorizované modifikaci informace, je narušena dostupnost, nikoli integrita. Z tohoto důvodu by bylo lépe definovat, že integrita je "prevence proti neodhalené neautorizované modifikaci informace". Změnou definice integrity by se dosáhlo jednoznačnějšího rozhraní mezi integritou a dostupností.

Při zavedení výše uvedené změny v definici integrity je možno navíc dosáhnout korespondence pojmů integrita a dostupnost s dobře definovanými pojmy z oblasti dokazování programů. Pojem integrita bude pak odpovídat pojmu částečná správnost (partial correctness) a pojmy integrita a dostupnost společně budou odpovídat pojmu úplná správnost (total correctness).

Kritika generických záhlaví definujících bezpečnostní funkcionalitu

Generická záhlaví pro funkce prosazující bezpečnost nejsou vytvořena systematicky a jejich výčet není úplný. Zvláště schází duální funkce k některým funkcím, prosazujícím bezpečnost. K identifikaci a autentizaci schází duální funkce *anonymita* a *pseudonymita*. Totéž platí o auditu a jeho duální funkci *nemožnost sledování* (Freeness from observability).

Zařazení funkce *výměna dat* mezi ostatní funkce prosazující bezpečnost je opět nesystematické, neboť tato funkce je na zcela jiné úrovni než funkce ostatní. Navíc chybí k ní odpovídající funkce *ukládání dat*. Klasifikace bezpečnostních funkcí by měla být doplněna tak, aby bylo umožněno hodnocení informačních systémů, které požadují nebo zajišťují *anonymitu*, *pseudonymitu* a *nemožnost sledování*.

Kritika příkladů tříd funkčnosti

Deset příkladů tříd funkčnosti, uvedených jako příloha dokumentu ITSEC, je pro uživatele dokumentu velmi nedostatečným materiálem. Uživatel má sice možnost definovat si své vlastní třídy funkčnosti, avšak pouze málo uživatelů je schopno tuto činnost provádět. Navíc uvedených deset příkladů tříd funkčnosti budí ve čtenáři mylný dojem, že tyto příklady tvoří kompletní a konzistentní sadu, pokrývající všechny problémy bezpečnosti.

3.5 Kanadská kritéria CTCPEC

Kanadská kritéria pro hodnocení bezpečnosti informačních systémů CTCPEC (Canadian Trusted Computer Product Evaluation Criteria, [CTCPEC]) zachovala dvourozměrný způsob hodnocení (tj. bezpečnostní funkčnost a zaručitelnost), ale pokusila se vytvořit prakticky použitelnější kategorizaci bezpečnostních funkcí. Je zde malá změna v terminologii – bezpečnostní funkce jsou v CTCPEC nazývány *bezpečnostními službami*. Tyto bezpečnostní funkce jsou rozděleny do čtyř kategorií: na bezpečnostní funkce zajišťující *důvěrnost*, *integritu*, *dostupnost* a *účtovatelnost*. V rámci každé bezpečnostní funkce je definováno několik *úrovní*. Úroveň bezpečnostní funkce je definovaný a měřitelný požadavek na granularitu nebo sílu bezpečnostní funkce vzhledem k určité množině hrozeb. Bezpečnostní funkce s vyšší úrovní poskytují účinnější ochranu proti hrozbám. Jednotlivé úrovně jsou hierarchické ve smyslu zvyšující se ochrany. To však neznamená, že následující úroveň musí nutně zahrnovat vše, co bylo požadováno v předchozích úrovních. Úrovně jsou vzestupně číslovány počínaje od nuly, která představuje nejnižší úroveň ochrany. Například bezpečnostní funkce *identifikace a autentizace*, která má zkratku WA, obsahuje úrovně WA-0, WA-1, WA-2 a WA-3.

Používané bezpečnostní funkce jsou následující:

- Bezpečnostní funkce zajišťující důvěrnost
  - Skryté kanály (obsahuje čtyři úrovně CC-0 až CC-3)
  - Nepovinné řízení důvěrnosti (CD-0 až CD-4)
  - Povinné řízení důvěrnosti (CM-0 až CM-4)
  - Opětné použití objektů (CR-0 až CR-1)
- Bezpečnostní funkce zajišťující integritu
  - Doménová integrita (IB-0 až IB-2)
  - Nepovinné řízení integrity (ID-0 až ID-4)
  - Povinné řízení integrity (IM-0 až IM-4)
  - Fyzická integrita (IP-0 až IP-4)
  - Návrat (IR-0 až IR-2)

- Oddělení rolí (IS-0 až IS-3)
- Autonomní testování (IT-0 až IT-3)

- Bezpečnostní funkce zajišťující dostupnost
  - Přidělování prostředků (AC-0 až AC-3)
  - Tolerance k chybám (AF-0 až AF-23)
  - Robustnost (AR-0 až AR-3)
  - Zotavení (AY-0 až AY-3)
- Bezpečnostní funkce zajišťující účtovatelnost
  - Audit (WA-0 až WA-5)
  - Identifikace a autentizace (WI-0 až WI-3)
  - Důvěryhodná cesta (WT-0 až WT-3)

Požadavky na míru záruky jsou v CTCPEC vyjádřeny pomocí tříd míry záruky, označených T0 až T7, přičemž T0 je třída rezervována pro systémy, které neprošly úspěšně hodnocením. Mezi třídami CTCPEC a ITSEC existuje relace, která je uvedena v následující tabulce:

ITSEC	CTCPEC
E0	T0
	T1
E1	T2
E2	T3
E3	T4
E4	T5
E5	T6
E6	T7

Tabulka 3.2 Vztah tříd míry záruky ITSEC a CTCPEC

Rozebírat vlastnosti kritérií CTCPEC detailněji asi není třeba. Ačkoli oficiální role těchto kritérií nepřesáhla hranice Kanady, šlo v době jejich vzniku o kritéria velmi moderní a dobře zpracovaná a jejich osvětový a didaktický význam je nesporný. Proto také tato kritéria sloužila jako jeden z podkladů pro tvorbu harmonizovaných mezinárodních kritérií CC, kterým se bude věnovat následující kapitola.

3.6 Kritéria bezpečnosti CC - ISO/IEC 15408

Tato kapitola se bude zabývat vysvětlením přístupu a filozofie nejnovějších kritérií pro hodnocení bezpečnosti informačních technologií, která jsou známa pod názvem Common

Criteria (CC, [CC]). Tato kritéria byla jako první z podobných kritérií přijata jako mezinárodní norma ISO/IEC 15408 a proto mají velkou šanci se stát jednotným a obecně respektovaným dokumentem, vhodným jak pro vývojáře, hodnotitele tak i pro uživatele bezpečných systémů informačních technologií.

3.6.1 Účel normy ISO/IEC 15408

Okruh čtenářů ISO/IEC 15408 zahrnuje spotřebitele, vývojáře a hodnotitele bezpečných systémů a produktů IT. Tyto skupiny mohou využít tuto část ISO/IEC 15408 následujícím způsobem:

- Spotřebitelé použijí ISO/IEC 15408 pří výběru komponent pro vyjádření svých bezpečnostních požadavků, které splní jejich bezpečnostní plán. Kapitola 4.3 dokumentu ISO/IEC 15408-1 poskytuje podrobnější informace o vztahu mezi bezpečnostní plánem a bezpečnostními požadavky
- Vývojáři, kteří reagují na skutečné nebo předpokládané bezpečnostní požadavky spotřebitelů při vývoji hodnoceného předmětu (HP), mohou v ISO/IEC 15408 nalézt standardizované metody pro porozumění požadavkům spotřebitelů. Mohou také využít obsah této části ISO/IEC 15408 jako základ pro definici bezpečnostní funkcí a mechanismů HP, které splňují tyto požadavky.
- Hodnotitelé využijí požadavky, definované v ISO/IEC 15408 při ověřování, zda HP splňují bezpečnostní plány a zda byly vzaty v úvahu všechny vzájemné závislosti a bylo ukázáno, že jsou splněny. Hodnotitelé by si také měli vzít tuto část ISO/IEC 15408 na pomoc při rozhodování, zda daný HP splňuje dané požadavky.

Požadavky na bezpečnost IT jsou konkretizací bezpečnostních plánů do množiny bezpečnostních požadavků na produkt nebo systém IT a na jeho prostředí. Produkt nebo systém IT může vyhovět svému bezpečnostnímu plánu, když jsou splněny požadavky na bezpečnost jeho prostředí. CC prezentují požadavky na bezpečnost IT ve dvou kategoriích. Stanovují se:

- *funkční požadavky* - požadavky na bezpečnostní funkcionalitu
- *požadavky zaručitelnosti bezpečnosti* - požadavky dané cílově požadovanou mírou zaručitelnosti bezpečnosti.

Požadavky na bezpečnostní funkcionalitu určují, která konkrétní bezpečnostní opatření (bezpečnostní funkce – identifikace, autentizace, bezpečnostní audit, nepopiratelnost původu apod.) se musí uplatnit, aby se podpořila bezpečnost produktu nebo systému IT.

Požadavky zaručitelnosti bezpečnosti mohou stanovovat sílu (odolnost) implementovaných bezpečnostních funkcí, požadované důkazy po hodnocení dodávané vývojářem, důkazy, které musí vypracovat třetí nezávislá strana (hodnotitel), rozsah, hloubku a přísnost hodnocení apod.

Záruka za splnění bezpečnostních plánů se odvozuje z dokázání oprávněnosti důvěry, že bezpečnostní funkce jsou implementovány správně a že implementované bezpečnostní funkce skutečně vyhovují daným bezpečnostním plánům.

3.6.2 Funkční požadavky a bezpečnostní funkce

Nyní se budeme zabývat bezpečnostními funkcemi, definovanými v mezinárodní normě ISO/IEC 15408, s názvem "*Informační technologie - Bezpečnostní techniky - Kritéria pro hodnocení bezpečnosti IT - Část 2: Bezpečnostní funkční požadavky*".

Bezpečnostní funkční komponenty, definované ve druhé části ISO/IEC 15408, jsou základem pro funkční požadavky bezpečnosti produktu nebo systému IT, vyjádřené v profilu ochrany (PO) a v bezpečnostním cíli (BC). Tyto požadavky popisují požadované bezpečnostní chování, očekávané od bezpečného produktu nebo systému IT a musí splňovat bezpečnostní plán, uvedený v PO nebo BC. Tyto požadavky popisují bezpečnostní vlastnosti, které mohou uživatelé pozorovat při jejich přímé interakci s produktem nebo systémem IT (tj. při jeho vstupních a výstupních operacích) a/nebo pozorováním odezvy produktu nebo systému IT na podnět.

Bezpečnostní funkční komponenty vyjadřují bezpečnostní požadavky, jejichž cílem je zabránit hrozbám v předpokládaném provozním prostředí produktu nebo systému IT nebo pokrýt všechny identifikované bezpečnostní politiky organizace nebo jiné předpoklady.

3.6.3 Rozšiřování a údržba funkčních požadavků

Norma ISO/IEC 15408 a její bezpečnostní funkční požadavky nejsou míněny jako definitivní odpověď na všechny problémy bezpečnosti IT. Norma naopak nabízí sadu srozumitelných bezpečnostních funkčních požadavků, které mohou být použity při vytváření důvěryhodných produktů nebo systémů, reflektujících požadavky trhu. Tyto bezpečnostní funkční požadavky jsou prezentovány jako současný stav poznání v oblasti specifikace požadavků a v oblasti hodnocení. Nepředpokládá se, že ISO/IEC 15408-2 obsahuje všechny možné bezpečnostní funkční požadavky, ale pouze ty, které jsou známé a na kterých se autoři normy v době vydání dokumentu dohodli, že jsou užitečné.

Jelikož se znalosti a potřeby spotřebitelů mohou měnit, funkční požadavky v této části ISO/IEC 15408 bude třeba dále modifikovat. Dá se předpokládat, že někteří autoři dokumentů *Profil ochrany* a *Bezpečnostní cíl* mohou mít bezpečnostní požadavky, které nejsou (doposud) pokryty třídami funkčních požadavků v ISO/IEC 15408-2. V těchto případech může autor dokumentu PO zvážit použití funkčních požadavků nepřevzatých z normy (takzvané rozšíření).

3.6.4 Organizace dokumentu ISO/IEC 15408-2

Kapitola 1 obsahuje úvodní materiál k ISO/IEC 15408-2. Kapitola 2 uvádí katalog funkčních komponent ISO/IEC 15408-2 a kapitoly 3 až 13 popisují jednotlivé funkční třídy.

Příloha A poskytuje dodatečné informace, které by mohly zajímat potenciální uživatele funkčních komponent, včetně úplné tabulky křížových referencí závislostí jednotlivých komponent. Přílohy B až M obsahují aplikační informace k jednotlivým funkčním třídám. Tyto přílohy jsou zdrojem podpůrných informací pro uživatele této části ISO/IEC 15408. Tyto informace jim mohou pomoci aplikovat relevantní činnosti a zvolit vhodné postupy pro audit a dokumentaci.

Autoři dokumentů PO a BC naleznou relevantní struktury, pravidla a návody v kapitole 2 dokumentu ISO/IEC 15408-1:

- ISO/IEC 15408-1, kapitola 2 definuje pojmy, použité v ISO/IEC 15408.

- ISO/IEC 15408-1, příloha B definuje strukturu profilu ochrany.
- ISO/IEC 15408-1, příloha C definuje strukturu bezpečnostního cíle.

3.6.5 Model funkčních požadavků

Nyní popíšeme model, použitý pro bezpečnostní funkční požadavky, uvedené v ISO/IEC 15408-2. Obrázky 3.1 a 3.2 zobrazují některé z klíčových konceptů modelu..

ISO/IEC 15408-2 je katalogem bezpečnostních funkčních požadavků, které mohou být předepsány pro *Hodnocený předmět (HP)*. HP je produkt nebo systém IT (spolu s uživateli a dokumentací pro správce), který obsahuje zdroje, jako jsou elektronická paměťová média (např. disky), periferní zařízení (např. tiskárny) a výpočetní kapacitu (např. čas CPU), které mohou být využity pro zpracování a ukládání informací. HP je předmětem hodnocení.

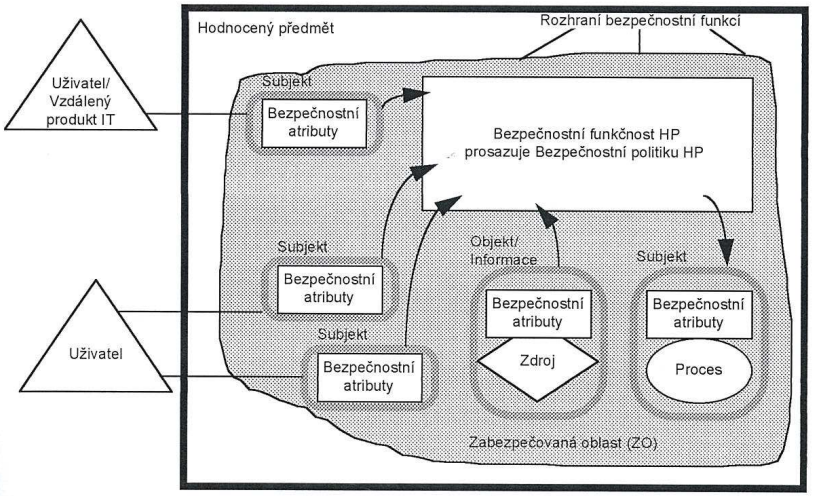
Hodnocení HP se soustřeďuje především na zajištění, že definovaná *Bezpečnostní politika HP (BPHP)* je prosazována pro všechny zdroje HP. BPHP definuje pravidla, pomocí kterých HP ovládá přístup ke svým zdrojům, a tím i ke všem informacím a službám, kontrolovaným HP.

BPHP se skládá z několika *Bezpečnostních politik bezpečnostních funkcí (BPBF)*. Každá BPBF má svůj rozsah působnosti, který definuje subjekty, objekty a operace, řízené touto politikou. BPBF je implementována pomocí *Bezpečnostní funkce (BF)*, jejíž mechanismy prosazují politiku a poskytují k tomu nezbytné schopnosti.

Ty části HP, na které se musíme spolehnout, aby byla prosazována BPHP, se společně nazývají *Bezpečnostní funkcionalita HP (BFHP)*. BFHP se skládá ze všeho hardwaru, softwaru a firmwaru HP, na kterém ať přímo, nebo nepřímo, závisí prosazení bezpečnosti.

HP může být monolitický produkt, obsahující hardware, firmware a software. Alternativně HP může být také distribuovaný produkt, který se interně skládá z několika oddělených částí. Každá z těchto částí HP poskytuje jistou službu pro HP a je propojena s ostatními částmi HP pomocí *interního komunikačního kanálu*. Tento kanál může být poměrně malý (jako například sběrnice procesoru) nebo může zahrnovat i interní počítačovou síť HP.

Pokud se HP skládá z několika částí, každá část HP může mít svou vlastní část BFHP, která si vyměňuje uživatelská data a data BFHP přes interní komunikační kanály s jinými částmi BFHP. Tato interakce se nazývá *přenos uvnitř HP*. V tomto případě oddělené části BFHP abstraktně tvoří složenou BFHP, která prosazuje BPHP.



Obr. 3.1 Model bezpečnostních funkčních požadavků (monolitický HP)

Rozhraní HP mohou být lokalizována uvnitř daného HP nebo mohou dovolit interakci s jinými produkty IT pomocí *externích komunikačních kanálů*. Tyto externí interakce s jinými produkty IT mohou mít dvojí formu:

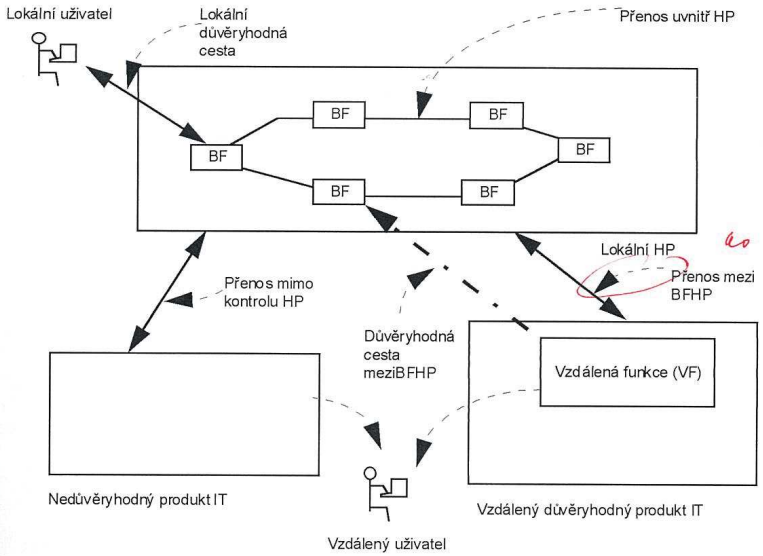
- Bezpečnostní politiky „vzdáleného důvěryhodného produktu IT" a BP lokálního HP byly administrativně navzájem koordinovány a ohodnoceny. V tomto případě je výměna informací nazývána *„přenos mezi BFHP"*, jelikož k ní dochází mezi BFHP různých důvěryhodných produktů.
- Vzdálený produkt IT nemusí být ohodnocen, což je naznačeno na obr. 3.2 jako „nedůvěryhodný produkt IT", tudíž jeho bezpečnostní politika je neznámá. Výměna informací je v tomto případě nazvána *"přenos mimo kontrolu BFHP"*, protože vzdálený produkt nemá žádnou BFHP (nebo charakteristika bezpečnostní politika je neznámá).

Sada interakcí, které se mohou vyskytnout uvnitř HP a které jsou subjektem pravidel BPHP, se nazývá *zabezpečovaná oblast (ZO)*. ZO zahrnuje definovanou sadu interakcí, založených na subjektech, objektech a operacích uvnitř HP, ale nemusí zahrnovat všechny zdroje HP.

Sada rozhraní, ať interaktivních (rozhraní člověk-stroj), nebo programátorských (aplikační programová rozhraní), pomocí kterých jsou zpřístupňovány zdroje spravované BFHP, nebo přes která jsou získávány informace z BFHP, se nazývá *rozhraní BFHP (RBFHP)*. RBFHP definuje hranice funkcí HP, které přispívají k prosazování BPHP.

Uživatelé jsou mimo HP, a tedy i mimo ZO. Pokud uživatelé požadují služby, poskytované HP, pracují s HP prostřednictvím RBFHP. Z hlediska funkčních požadavků ISO/IEC 15408-2 existují dva typy uživatelů: *osoby* a *externí entity IT*. Osoby se dále dělí na *lokální uživatele*, kteří přímo interagují s HP prostřednictvím určitých zařízení HP (např. prostřednictvím

pracovních stanic) a na *vzdálené uživatele*, kteří interagují s HP nepřímo prostřednictvím jiného produktu IT.



Obr. 3.2 Diagram bezpečnostních funkcí v distribuovaném HP

Časový interval interakce mezi uživateli a BFHP se nazývá *relace* uživatele. Vytvoření relace může být podmíněno různými okolnostmi, např. autentizací uživatele, hodinou, metodou přístupu k HP nebo maximálním povoleným počtem relací uživatele. Tato část ISO/IEC 15408 používá pojem *autorizovaný* pro označení uživatele, který vlastní práva a/nebo privilegia nezbytná pro provedení dané operace. Pojem *autorizovaný uživatel* tedy označuje, že BPHP tomuto uživateli povoluje provést danou operaci.

HP obsahuje zdroje, které mohou být použity pro zpracování a ukládání informací. Primární cíl BFHP je úplné a správné prosazení BPHP nad zdroji a informacemi, které HP spravuje. Zdroje HP mohou být strukturovány a využity mnoha různými způsoby. ISO/IEC 15408-2 používá rozlišení, které umožňuje specifikaci požadovaných bezpečnostních vlastností.

Všechny entity, které mohou být vytvořeny ze zdrojů, mohou být dvou druhů. Entity mohou být aktivní, což znamená, že jsou příčinou akcí uvnitř HP a zapříčiňují operace, které jsou prováděny nad informacemi. Na druhé straně mohou být entity pasivní, což znamená, že jsou kontejnerem, ze kterého informace pocházejí nebo do kterého jsou informace uloženy.

Aktivní entity se nazývají *subjekty*. Uvnitř HP může existovat několik druhů subjektů:

- Ty, které pracují pod kontrolou autorizovaného uživatele a které jsou subjektem všech pravidel BPHP (např. procesy v UNIXu).
- Ty, které pracují jako speciální funkční procesy, které mohou pracovat v zájmu mnoha uživatelů (např. funkce, které se nacházejí v architekturách klient/server).

- Ty, které jsou samotnou součástí HP (např. důvěryhodné procesy).

Nad těmito typy subjektů popisuje ISO/IEC 15408-2 prosazování BPHP.

Pasivní entity (např. kontejnery s informacemi) jsou v bezpečnostních funkčních požadavcích ISO/IEC 15408-2 nazývány *objekty*. Objekty jsou cílem operací, které jsou prováděny subjekty. V případě, že subjekt (aktivní entita) je cílem operace (například meziprocesové komunikace), může subjekt vystupovat jako objekt. Objekty mohou obsahovat *informace*.

3.6.6 Katalog komponent funkčních požadavků

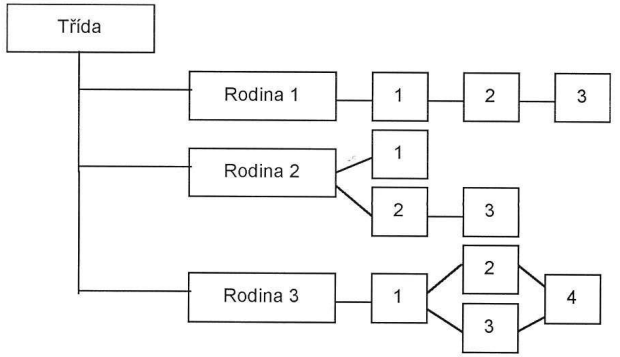
Seskupení komponent funkčních požadavků v ISO/IEC 15408-2 neodpovídá žádné formální taxonomii. Bezpečnostní funkce jsou rozděleny do kategorií, které se nazývají *třídy* (např. třída Bezpečnostní audit nebo třída Komunikace). Každá třída se skládá z *rodin*, které odpovídají např. bezpečnostním funkcím v kritériích CTCPEC. Konečně každá rodina se skládá z *komponent*, které plní požadavky rodiny s různou mírou ochrany. Na rozdíl od kritérií CTCPEC nemusí být jednotlivé komponenty nutně hierarchické.

Katalog funkčních požadavků obsahuje třídy rodin a komponent, které jsou pouhým seskupením podle podobné funkce nebo podobného účelu a komponenty v rámci třídy jsou uvedeny v abecedním pořadí. Katalog obsahuje následující třídy:

- Třída *FAU*: Bezpečnostní audit
- Třída *FCO*: Komunikace
- Třída *FCS*: Kryptografická podpora
- Třída *FDP*: Ochrana uživatelských dat
- Třída *FIA*: Identifikace a autentizace
- Třída *FMT*: Správa bezpečnosti
- Třída *FPR*: Soukromí
- Třída *FPT*: Ochrana bezpečnostní funkcionality
- Třída *FRU*: Využití zdrojů
- Třída *FTA*: Přihlášení do HP
- Třída *FTP*: Důvěryhodné cesty/kanály

Na začátku každé třídy je uveden v dokumentu ISO/IEC 15408-2 informativní diagram, který ukazuje strukturu této třídy, rodiny v této třídě a komponenty v každé rodině. Tento diagram je užitečný pro objasnění vztahů, které mohou existovat mezi jednotlivými komponentami.

V každé třídě je v dokumentu ISO/IEC 15408-2 uveden obrázek ilustrující hierarchii rodiny, podobný obr. 3.3.



Obr. 3.3 Ukázka rozdělení třídy na rodiny a komponenty

Na obr. 3.3 je první rodinou rodina 1, která obsahuje tři hierarchické komponenty. Komponenta 2 a komponenta 3 mohou obě splňovat požadavky komponenty 1. Stejně tak komponenta 3 může splňovat požadavky komponenty 2. V rodině 2 jsou tři komponenty, které nejsou všechny navzájem hierarchické. Komponenta 3 může splňovat požadavky komponenty 2, avšak nemůže splňovat požadavky komponenty 1.

V následujících kapitolách si ukážeme přehled jednotlivých tříd a rodin, definovaných v katalogu funkčních požadavků ISO/IEC 15408-2. Vzhledem ke značnému počtu komponent v katalogu zde nemůžeme uvést přehled komponent – zájemce odkazujeme na dokument ISO/IEC 15408-2.

Třída FAU: Bezpečnostní audit

Bezpečnostní audit zahrnuje rozpoznávání, zaznamenávání, ukládání a analyzování informací, které mají vztah k aktivitám, významným z hlediska bezpečnosti (tj. aktivitám, pokrytým bezpečnostní politikou). Výsledné auditní záznamy mohou být následně zkoumány, aby se zjistilo, které bezpečnostně významné aktivity se staly a kdo (který uživatel) je za ně zodpovědný. Třída bezpečnostních funkcí Bezpečnostní audit obsahuje tyto rodiny komponent:

- FAU-ARP Automatická reakce bezpečnostního auditu
- FAU-GEN Generování dat bezpečnostního auditu
- FAU-SAA Analýza bezpečnostního auditu
- FAU-SAR Kontrola bezpečnostního auditu
- FAU-SEL Výběr událostí bezpečnostního auditu
- FAU-STG Ukládání událostí bezpečnostního auditu

Třída FCO: Komunikace

Tato třída obsahuje dvě rodiny, které se zabývají bezpečným zjištěním identity protistrany, která se účastní výměny (přenosu) dat. Tyto rodiny se vztahují k zajištění identity původce

přenášené informace (důkaz původu) a k zajištění identity příjemce přenášené informace (důkaz přijetí). Zajišťují, že ani původce nemůže popřít odeslání zprávy, ani příjemce nemůže popřít její přijetí. Třída bezpečnostních funkcí Komunikace obsahuje tyto rodiny komponent:

- FCO-NRO Nepopiratelnost původu
- FCO-NRR Nepopiratelnost přijetí

Třída FCS: Kryptografická podpora

BFHP může zahrnovat i kryptografické funkce, které pomohou splnit některé bezpečnostní plány vyšší úrovně. Tyto plány zahrnují (mimo jiné): identifikaci a autentizaci, nepopiratelnost, důvěryhodnou cestu, důvěryhodný kanál a oddělení dat. Tato třída se použije, pokud HP obsahuje kryptografické funkce, jejichž implementace může být provedena pomocí hardwaru, firmwaru a/nebo softwaru.

Třída FCS se skládá ze dvou rodin: FCS-CKM Správa kryptografických klíčů a FCS-COP Kryptografické operace. Rodina FCS-CKM se zabývá aspekty správy kryptografických klíčů, zatímco rodina FCS-COP se zabývá jejich provozním použitím.

- FCS-CKM Správa kryptografických klíčů
- FCS-COP Kryptografické operace

Třída FDP: Ochrana uživatelských dat

Tato třída obsahuje rodiny, definující požadavky na bezpečnostní funkce HP a bezpečnostní politiky HP, které se vztahují k ochraně uživatelských dat. Třída FDP se dělí na čtyři skupiny rodin, které se starají o uživatelská data uvnitř HP během jejich importu, exportu a uložení a o bezpečnostní atributy, které se přímo vztahují k uživatelským datům. Rodiny třídy FDP se dělí na následující čtyři skupiny:

a) Bezpečnostní politiky bezpečnostních funkcí ochrany uživatelských dat

- FDP-ACC Politika řízení přístupu
- FDP-IFC Politika řízení toku informace

Komponenty v těchto rodinách umožňují, aby autor profilu ochrany nebo bezpečnostního cíle definoval bezpečnostní politiky bezpečnostních funkcí týkajících se ochrany uživatelských dat a definoval rozsah působnosti politik, nutný pro stanovení bezpečnostních plánů. Názvy těchto politik by měly být použity v ostatních funkčních komponentách, jejichž činnost je vyžadována v „bezpečnostní politice řízení přístupu“ nebo v „bezpečnostní politice řízení toku informace“. Pravidla, definující funkčnost vyjmenovaných politik řízení přístupu a řízení toku dat, budou definována v rodinách FDP-ACF a FDP-IFF.

b) Jednotlivé způsoby ochrany uživatelských dat

- FDP-ACF Funkce řízení přístupu
- FDP-IFF Funkce řízení toku informace
- FDP-ITT Přenos uvnitř HP
- FDP-RIP Ochrana zbytkových informací

- FDP-ROL Odvolání operace (rollback)
- FDP-SDI Integrita uložených dat

c) Off-line uložení, import a export dat

- FDP-DAU Autentizace dat
- FDP-ETC Export mimo oblast řízení TSF
- FDP-ITC Import z oblasti mimo řízení TSF

Komponenty v těchto rodinách se zabývají důvěryhodným přenosem do a ze zabezpečované oblasti.

d) Přenos mezi BFHP

- FDP-UCT Ochrana důvěrnosti uživatelských dat při přenosech mezi BFHP
- FDP-UIT Ochrana integrity uživatelských dat při přenosech mezi BFHP

Komponenty v těchto rodinách se zabývají přenosem mezi BFHP a jiným důvěryhodným produktem IT.

Třída FIA: Identifikace a autentizace

Rodiny v této třídě se zabývají požadavky na funkce, které zjišťují a ověřují identitu uživatele.

Identifikace a autentizace jsou nutné k tomu, aby bylo zajištěno, že uživateli jsou přiřazeny odpovídající bezpečnostní atributy (tj. například jeho identita, příslušnost ke skupinám uživatelů, role, bezpečnostní úrovně integrity).

Jednoznačná identifikace autorizovaných uživatelů a správné přiřazení bezpečnostních atributů uživatelům a subjektům je z hlediska prosazení bezpečnostních politik kritická. Tato rodina se ve svých třídách zabývá určením a verifikací identity jednotlivých uživatelů, určením jejich oprávnění k interakci s HP a správným přiřazením bezpečnostních atributů každému autorizovanému uživateli. Některé jiné třídy požadavků (např. ochrana uživatelských dat a bezpečnostní audit) jsou pro svou efektivní činnost závislé na správné identifikaci a autentizaci uživatelů. Třída bezpečnostních funkcí Identifikace a autentizace obsahuje tyto rodiny komponent:

- FIA-AFL Obsluha neúspěšné autentizace
- FIA-ATD Definice atributů uživatele
- FIA-SOS Specifikace tajemství
- FIA-UAU Autentizace uživatele
- FIA-UID Identifikace uživatele
- FIA-USB Vazba uživatel-subjekt

Třída FMT: Správa bezpečnosti

Cílem této třídy je specifikovat správu některých aspektů BFHP: bezpečnostních atributů, dat BFHP a funkcí BFHP. Mohou zde být také specifikovány různé role správců a jejich vztahy,

jako je např. oddělení pravomocí. Třída bezpečnostních funkcí Správa bezpečnosti obsahuje tyto rodiny komponent:

- FMT-MOF Správa funkcí BFHP
- FMT-MSA Správa bezpečnostních atributů
- FMT-MTD Správa dat BFHP
- FMT-REV Odvolání bezpečnostních atributů
- FMT-SAE Vypršení platnosti bezpečnostních atributů
- FMT-SMR Role správy bezpečnosti

Třída FPR: Soukromí

Tato třída obsahuje požadavky na zachování soukromí uživatelů. Požadavky v této třídě poskytují ochranu uživatele před zjištěním jeho identity a zneužitím jeho identity jinými uživateli. Třída Soukromí zahrnuje následující rodiny:

- FPR-ANO Anonymita
- FPR-PSE Pseudonymita
- FPR-UNL Nespojitelnost
- FPR-UNO Nepozorovatelnost

Třída FPT: Ochrana bezpečnostní funkcionality

Tato třída obsahuje rodiny funkčních požadavků, které se vztahují k integritě a správě mechanismů, které poskytuje BFHP (nezávisle na specifikách BPHP) pro zajištění integrity dat BFHP (nezávisle na specifickém obsahu dat BPHP). V jistém smyslu se mohou rodiny v této třídě zdát duplicitní ke komponentám ve třídě FDP (ochrana uživatelských dat). Je dokonce možné, že tyto funkce mohou být implementovány pomocí stejných mechanismů. Rozdíl je však v tom, že FDP se soustředí na ochranu uživatelských dat, zatímco FPT se soustředí na ochranu dat BFHP. Komponenty třídy FPT jsou nezbytné k tomu, aby existovaly požadavky na to, že BPBF v HP nemohou být narušeny nebo obejity.

Z hlediska této třídy se BFHP skládá ze tří významných částí:

- Z *abstraktního stroje* BFHP, který je virtuálním nebo fyzickým strojem, na němž běží hodnocené implementace BFHP.
- Z *implementace* BFHP, která běží na abstraktním stroji a implementuje mechanismy, které prosazují BPHP.
- Z *dat* BFHP, která tvoří administrační databázi, jež řídí prosazování BPHP.

Pro ochranu těchto tří částí nabízí třída bezpečnostních funkcí Ochrana bezpečnostní funkcionality tyto rodiny komponent:

- FPT-AMT Testování abstraktního stroje
- FPT-FLS Bezpečnost při výpadku
- FPT-ITA Dostupnost exportovaných dat BFHP
- FPT-ITC Důvěrnost exportovaných dat BFHP

- FPT-ITI Integrita exportovaných dat BFHP
- FPT-ITT Přenos dat BFHP uvnitř HP
- FPT-PHP Fyzická ochrana BFHP
- FPT-RCV Důvěryhodná obnova
- FPT-RPL Detekce přehrání
- FPT-RVM Zprostředkování odkazů
- FPT-SEP Oddělení domén
- FPT-SSP Protokol synchronizace stavu
- FPT-STM Časové známky
- FPT-TDC Konzistence dat BFHP mezi BFHP
- FPT-TRC Konzistence replikace dat BFHP uvnitř BFHP
- FPT-TST Autonomní testování BFHP

Třída FRU: Využití zdrojů

Tato třída obsahuje tři rodiny, které podporují dostupnost požadovaných zdrojů, jako je výpočetní kapacita nebo kapacita uložení dat. Rodina Tolerance k chybám poskytuje ochranu proti nedostupnosti kapacit, způsobených výpadkem HP. Rodina Priorita služeb zajišťuje, že zdroje budou přednostně přidělovány důležitějším nebo časově kritickým úlohám a že si je nebudou moci monopolizovat úlohy s nižší prioritou. Rodina Alokace zdrojů zajišťuje limity na využití dostupných zdrojů a tím zabraňuje uživatelům v monopolizaci zdrojů.

- FRU-FLT Tolerance k chybám
- FRU-PRS Priorita služeb
- FRU-RSA Alokace zdrojů

Třída FTA: Přihlášení do HP

Tato třída specifikuje funkční požadavky na kontrolu ustavení uživatelské relace. Obsahuje tyto rodiny komponent:

- FTA - LSA Omezení rozsahu volitelných atributů
- FTA -MCS Omezení vícenásobných současných relací
- FTA -SSL Uzamykání relace
- FTA-TAB Varování při přihlášení
- FTA -TAH Historie přihlášení
- FTA -TSE Ustavení relace

Třída FTP: Důvěryhodné cesty/kanály

Rodiny komponent v této třídě obsahují požadavky na důvěryhodnou komunikační cestu mezi uživateli a BFHP a pro důvěryhodný komunikační kanál mezi BFHP a jinými důvěryhodnými produkty IT. Důvěryhodné cesty a kanály mají tyto obecné vlastnosti:

- Komunikační cesta je vytvořena pomocí interních a externích komunikačních kanálů (podle typu komponenty), které izolují definovanou podmnožinu dat a příkazů BFHP od zbytku BFHP a uživatelských dat.
- Použití komunikační cesty může být iniciováno uživatelem anebo BFHP (podle typu komponenty).
- Komunikační cesta je schopna poskytnout záruku, že uživatel komunikuje se správnou BFHP a že BFHP komunikuje se správným uživatelem (podle typu komponenty).

Důvěryhodný kanál je v tomto modelu komunikační kanál, který může být iniciován na jednom z jeho konců a poskytuje vlastnost "nepopiratelnost identity stran" na jeho koncích.

Důvěryhodná cesta poskytuje uživatelům prostředky pro provádění činností se zaručením přímé interakce s BFHP. Je obvykle požadována pro některé akce uživatele, jako je počáteční identifikace a autentizace, může však být vyžadována i v jiných okamžicích v průběhu relace. Důvěryhodná cesta může být iniciována buď uživatelem nebo BFHP. Je zaručeno, že příkazy uživatele, jdoucí přes důvěryhodnou cestu, jsou chráněny před modifikací a prozrazením nedůvěryhodným aplikacím.

Tato třída zahrnuje následující rodiny:

- FTP-ITC Důvěryhodný kanál mezi BFHP
- FTP-TRP Důvěryhodná cesta

3.6.7 Úrovně zaručitelnosti bezpečnosti podle CC

Kritéria, stanovená normou ISO/IEC 15408, definují vzrůstající škálu úrovní zaručitelnosti bezpečnosti. Jednotlivé úrovně definované na této škále jsou zavedeny tak, aby se dosáhlo vyrovnaného vztahu mezi *úrovní zaručitelnosti bezpečnosti* na straně jedné a cenou a realizovatelností požadovanou takovým stupněm zaručitelnosti na straně druhé.

Definice jednotlivých úrovní záruk za bezpečnost uvádějí, které požadavky zaručitelnosti bezpečnosti musí být splněny na jednotlivých úrovních.

Definovaných *úrovní zaručitelnosti bezpečnosti*, *EAL* (Evaluation Assurance Level), je sedm. Jsou uspořádané hierarchicky, každá úroveň musí splňovat jednak požadavky zaručitelnosti všech nižších úrovní a navíc požadavky definované na dané úrovni zaručitelnosti nově. Pro konkrétní aplikační prostředí se mohou jednotlivé úrovně zaručitelnosti bezpečnosti volitelně zesilovat.

Závěrem uvádíme konkrétní základní charakteristiky jednotlivých úrovní zaručitelnosti bezpečnosti (EAL) podle normy ISO/IEC 15408.

EAL1, funkčně testovaný produkt nebo systém IT

Úroveň EAL1 je použitelná tam, kde se požaduje správný (bezchybný) provoz, ale hrozby nejsou posuzovány jako závažné. Je vhodná tehdy, když se požaduje získání nezávisle vyslovené záruky podporující tvrzení, že byla vynaložena patřičná snaha o ochranu např. personalistik a podobných informací.

Úroveň EAL1 se odvozuje z hodnocení produktu nebo systému IT dostupného zákazníkovi. Hodnocení zahrnuje nezávislé testování, zda jsou splněny specifikace a zkoumání poskytnuté

dokumentace s návody. Hodnocení na této úrovni by mohlo být úspěšně proveditelné bez spoluúčasti a bez pomoci vývojáře a mohlo by si vyžádat vynaložení minimálních nákladů.

Při hodnocení produktu nebo systému IT úrovně EAL1 se poskytují důkazy, že jeho funkčnost je konzistentní s dokumentací a že poskytuje použitelnou ochranu proti identifikovaným hrozbám.

EAL2, strukturálně testovaný produkt nebo systém IT

Na úrovni EAL2 se požaduje kooperace s vývojářem, pro hodnocení jsou od vývojáře požadovány informace o návrhu a výsledky testů. Po vývojáři se ovšem nemá požadovat více než odpovídá dobrým obchodním praktikám, hodnocení si tudíž neklade požadavky na podstatné zvýšení finančních a časových nákladů.

Úroveň EAL2 je proto vhodnou úrovní pro podmínky, ve kterých vývojář nebo uživatel požadují malou až průměrnou úroveň nezávisle zaručované bezpečnosti a nepožaduje se dostupnost úplné vývojové dokumentace. Tato situace může odpovídat např. zabezpečování systémů podnikového účetnictví nebo případům, kdy je vývojář dostupný pouze omezeně.

EAL3, metodicky testovaný a kontrolovaný produkt nebo systém

Úroveň EAL3 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti odvozenou z průkazného používání bezpečnostního konstruování při návrhu produktu nebo systému IT, a to aniž by vývojář musel podstatně měnit své dobré vývojové praktiky.

Úroveň EAL3 je vhodná pro podmínky, ve kterých vývojář nebo uživatel požadují průměrnou úroveň nezávisle zaručené bezpečnosti, důkladné vyšetření produktu nebo systému IT a vývoje a nechtějí provádět rozsáhlý reengineering.

EAL4, metodicky navrhovaný, testovaný a přezkoumávaný produkt nebo systém IT

Úroveň EAL4 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti, odvozenou z průkazně používaného bezpečnostního inženýrství založeného na dobrých komerčních vývojových praktikách, které, třebaže se požaduje vysoká přísnost, nepožadují mimořádně velké odborné znalosti, dovednosti a jiné zdroje. Úroveň EAL4 je nejvyšší úrovní zaručitelnosti bezpečnosti, která bude muset pravděpodobně být ekonomicky zabudovatelná do existujících výrobních postupů.

Úroveň EAL4 je tudíž vhodná pro podmínky, ve kterých vývojář nebo uživatel požadují průměrnou až vysokou úroveň nezávisle zaručené bezpečnosti pro běžně prodávané zboží a jsou srozuměni s vynaložením dodatečných nákladů na specifické bezpečnostní konstruování.

EAL5, poloformálně navrhovaný a testovaný produkt nebo systém IT

Úroveň EAL5 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti odvozenou z průkazně používaného bezpečnostního konstruování založeného na dokonalých komerčních vývojových praktikách podporovaných běžnou, nikoli extrémní aplikací speciálních bezpečnostních technik. Takový produkt nebo systém IT bude pravděpodobně navrhován a vyvíjen s apriorním záměrem dosažení úrovně zaručitelnosti bezpečnosti EAL5. Je pravděpodobné, že dodatečné náklady vynaložené na splnění podmínek

zaručitelnosti bezpečnosti EAL5, při porovnání s použitím náročných vývojových postupů bez zahrnování specializovaných technik, nebudou velké.

Úroveň EAL5 je tudíž vhodná pro podmínky, ve kterých vývojář nebo uživatel požadují vysokou úroveň nezávisle zaručené bezpečnosti pro speciálně plánovaný vyvíjený produkt nebo systém IT a požadují použití dokonalých vývojových nástrojů a nechtějí hradit neodůvodněně zvýšené náklady za použití speciálních bezpečnostních technik.

EAL6, testovaný produkt nebo systém IT se poloformálně ověřovaným návrhem

Úroveň EAL6 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti odvozenou z prokázaného použití bezpečnostního konstruování a dokonalého vývojové prostředí. Cílem je mít možnost vytvářet vynikající produkty nebo systémy IT pro ochranu aktiv s vysokou hodnotou provozované ve vysoce rizikových prostředích.

Úroveň EAL6 je tudíž vhodná pro vývoj bezpečných produktů nebo systémů IT, které se mají používat ve vysoce rizikových prostředích a kde hodnota chráněných aktiv ospravedlňuje dodatečné vyšší náklady.

EAL7, testovaný produkt nebo systém IT s formálně ověřovaným návrhem

Úroveň bezpečnosti EAL7 se používá pro vývoj bezpečných produktů nebo systémů IT určených pro provozování ve vysoce rizikových prostředích nebo kde vysoká hodnota aktiv ospravedlňuje vyšší náklady. Praktická použitelnost EAL7 je v současné době omezena na produkty nebo systémy IT s úzce zaměřenou bezpečnostní funkcionalitou, kterou lze rozsáhle formálně analyzovat.

Jak lze očekávat, úrovně zaručitelnosti podle CC lze vyjádřit v pojmech jiných kritérií. Proto ukážeme tabulku vztahu těchto úrovní s třídami míry záruky jiných kritérií:

CC	TCSEC	ITSEC	CTCPEC
-	D	E0	T0
EAL1	-	-	T1
EAL2	C1	E1	T2
EAL3	C2	E2	T3
EAL4	B1	E3	T4
EAL5	B2	E4	T5
EAL6	B3	E5	T6
EAL7	A1	E6	T7

Tabulka 3.3 Vztah úrovní zaručitelnosti CC k TCSEC, ITSEC a CTCPEC

Úrovně zaručitelnosti podle CC by si zasloužily přinejmenším stejně rozsáhlý výklad jako již vysvětlené třídy funkčnosti. Zde se jimi ale nebudeme do větší hloubky zabývat, protože zaručitelnosti podle CC je věnována podstatná část kapitoly 5.

4 Doplňková kritéria

Při hodnocení bezpečnosti informačních systémů nevystačíme vždy pouze se zvolenými kritérii pro hodnocení bezpečnosti informačních systémů. Existuje totiž několik oblastí, kterým se kritéria více či méně vyhýbají. Důvody, proč tomu tak je, jsou různé. Někdy jde o důvody historické, jindy o důvody politické nebo profesní. V běžné praxi se dají identifikovat asi tři hlavni oblasti, kde je třeba při hodnocení bezpečnosti informačních systémů použít doplňkových kritérií nebo standardů. Jde o zabezpečení přenosu dat, o hodnocení kryptografických modulů a o hodnocení procesů managementu bezpečnosti. Tento výčet samozřejmě není úplný a u většiny systémů je třeba mít k dispozici ještě další, specializované standardy, avšak výše uvedené tři oblasti jsou pro mnoho systémů společné. Proto pro každou z těchto oblastí uvedeme příklad typického standardu, který se při hodnocení bezpečnosti používá.

4.1 Kritéria pro zabezpečení přenosu dat

V historii vývoje kritérií pro hodnocení bezpečnosti IS se stalo téměř pravidlem, že se tato kritéria téměř nezabývají bezpečnostními aspekty komunikace a přenosu dat. Některá kritéria se této oblasti vyhýbají úplně, jiná ji řeší vágní definicí kategorií a požadují, aby se bezpečnostní aspekty přenosu dat řešily pomocí jiného standardu. Tímto standardem v praxi většinou bývá mezinárodní norma ISO 7498-2 ISO/OSI Security Architecture ([ISO7498]), která definuje *základní bezpečnostní služby pro komunikační sítě*. Norma ISO 7498-2, vydaná rovněž jako doporučení mezinárodní telekomunikační unie ITU-T X.800, se zabývá bezpečnostní architekturou otevřených systémů, zavádí standardní definice termínů z bezpečnosti IT, uvádí standardní popisy bezpečnostních funkcí a bezpečnostních mechanismů, definuje, ve které vrstvě hierarchicky uspořádané architektury OSI lze bezpečnostní funkce poskytovat a zavádí pojem *správy bezpečnosti*.

4.1.1 Bezpečnostní služby v počítačových sítích

Norma ISO 7498-2 *ISO/OSI Security Architecture* definuje základní bezpečnostní služby pro komunikační sítě. Bezpečnostní služby, popsané v normě, mohou být v praxi implementovány na různých vrstvách komunikačního protokolu. V souladu s normou ISO/OSI budeme bezpečnostní služby dělit do následujících skupin: služby pro autentizaci, služby pro řízení přístupu, služby pro zajištění důvěrnosti, služby pro zajištění integrity a služby pro nepopiratelnost.

Autentizace

V počítačových sítích je mnoho typů subjektů, které musí nebo mohou být identifikovány a autentizovány. Jde především o fyzické subjekty (například uzly sítě, směrovače atd.), logické subjekty (typicky procesy) a lidské subjekty (např. uživatele a správce). *Identifikací* rozumíme určení jednoznačné identity subjektu bez jejího ověřování. *Autentizací* rozumíme ověření proklamované identity subjektu.

Služby pro autentizaci mají za úkol provádět autentizaci (ověření totožnosti) jedné nebo obou stran při komunikaci. Služby pro autentizaci se dělí na služby *Autentizace odesílatele* a služby

Autentizace spojení. Služby *Autentizace odesílatele* autentizují pouze odesílatele zprávy a nemusí poskytovat ochranu před duplikováním zpráv útočníkem. Služby *Autentizace spojení* poskytují autentizaci platnou během celého navázaného spojení a zabraňují duplikování zpráv útočníkem.

Služby pro řízení přístupu

Služby poskytující *Řízení přístupu* zajišťují ochranu před neautorizovaným použitím prostředků, dostupných prostřednictvím distribuovaného systému. Tyto služby však bývají málokdy součástí síťových protokolů a často jsou implementovány až v operačním systému nebo aplikaci.

Služby pro zajištění důvěrnosti

Tato skupina služeb poskytuje ochranu přenášených dat před neautorizovaným odhalením. Služba pro *Důvěrnost přenosu zpráv* poskytuje ochranu před neautorizovaným odhalením bez ohledu na navázaná spojení. Proto je tato služba vhodná pro bezkontextové aplikace. Služba pro *Důvěrnost spojení* zajišťuje ochranu před neautorizovaným odhalením v rámci navázaného spojení. Tato služba vyžaduje navázání spojení. Služba *Důvěrnost toku dat* (Traffic Flow Confidentiality) má za úkol zabránit útočníkovi, aby ze znalosti toku dat (adresy přenášených zpráv, délky přenášených zpráv, časové intervaly mezi přenášenými zprávami atd.) dokázal odvodit důvěrné informace o přenášených datech. Služba *Selektivní důvěrnost* má za úkol zajistit důvěrnost pouze některých částí přenášené zprávy.

Služby pro zajištění integrity

Tato skupina služeb poskytuje ochranu přenášených dat před neautorizovanou modifikací. Služba *Integrita přenosu zpráv* poskytuje ochranu před neautorizovanou modifikací bez ohledu na navázaná spojení. Služba *Integrita spojení* zajišťuje ochranu před neautorizovanou modifikací v rámci navázaného spojení. Tato služba vyžaduje navázání spojení. Služby *Selektivní integrita spojení* a *Selektivní integrita zpráv* mají za úkol zajistit integritu pouze některých částí přenášené zprávy.

Služby pro nepopiratelnost

Služby *Nepopiratelnost odesílatele* a *Nepopiratelnost doručení* slouží k tomu, aby příjemce (odesílatel) mohl prokázat protistraně odeslání (přijetí) zprávy a tím zabránil pozdějšímu popření této akce protistranou.

4.1.2 Implementace bezpečnostních služeb v jednotlivých vrstvách OSI

Jednotlivé vrstvy RM OSI v sestupném pořadí plní následující funkce:

- Vrstva 7 – *aplikační*: poskytuje aplikačně orientované služby.
- Vrstva 6 – *prezentační*: koordinuje kódování a syntaxi vyměňovaných dat.
- Vrstva 5 – *relační*: poskytuje pro IS nástroje pro řízení a synchronizaci jejich dialogů.
- Vrstva 4 – *transportní*: zvyšuje kvalitu komunikačních spojů na požadovanou úroveň.

- Vrstva 3 – *síťová*: směruje tok dat komunikačními spoji sítě. Data jsou za účelem směrování a přenosu komunikačními spoji organizována do paketů.
- Vrstva 2 – *spojová*: organizuje telekomunikační provoz po datovém spoji; prostý proud bitů přenášený fyzickou vrstvou mění na spolehlivou cestu přenosu bloků dat (rámců).
- Vrstva 1 – *fyzická*: přenáší prostý proud bitů přenosovým médiem.

Následující tabulka ukazuje, ve kterých vrstvách referenčního modelu ISO OSI by měly být jednotlivé bezpečnostní služby implementovány. V této tabulce písmeno A znamená, že tato vrstva je vhodná pro implementaci odpovídající bezpečnostní služby. Z tabulky je zřejmé, že samotná aplikační vrstva 7 může teoreticky implementovat všechny bezpečnostní služby. Z ostatních vrstev jsou nejvhodnější pro implementaci bezpečnostních funkcí vrstvy 3 a 4.

	Vrstva, na které může být služba zajišťována						
Bezpečnostní služba	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Autentizace spojení			A	A			A
Autentizace odesílatele			A	A			A
Řízení přístupu			A	A			A
Důvěrnost spojení	A	A	A	A		A	A
Důvěrnost přenosu zpráv		A	A	A		A	A
Selektivní důvěrnost						A	A
Důvěrnost toku dat	A		A				A
Integrita spojení s opravou				A			A
Integrita spojení bez opravy			A	A			A
Selektivní integrita spojení							A
Integrita přenosu zpráv			A	A			A
Selektivní integrita zpráv							A
Nepopiratelnost odeslání							A
Nepopiratelnost doručení							A

Tabulka 4.1 Přiřazení bezpečnostních služeb vrstvám ISO OSI

V dokumentech ISO jsou kromě výše uvedeních bezpečnostních služeb také definovány bezpečnostní mechanismy, kterými se služby mají implementovat. Jedná se o následující mechanismy:

- šifrování (kryptografické zabezpečení)
- elektronický podpis
- mechanismy řízení přístupu
- integritní mechanismy (kryptografické)
- kryptografická autentizace
- zarovnávání zpráv
- řízení směrování
- notářské služby

Přiřazení bezpečnostních mechanismů jednotlivým službám je následující:

Mechanismus Služba	Šifrování	El. podpis	Řízení přístupu	Integritní mecha-nismy	Krypt. autenti-zace	Zarovná-vání zpráv	Řízení směro-vání	Notářské služby
Autentizace spojení	A	A			A			
Autentizace odesílatele	A	A						
Řízení přístupu			A					
Důvěrnost spojení	A						A	
Důvěrnost přenosu zpráv	A						A	
Selektivní důvěrnost	A							
Důvěrnost toku dat	A					A	A	
Integrita spojení s opravou	A			A				
Integrita spojení bez opravy	A			A				
Selektivní integrita spojení	A			A				
Integrita přenosu zpráv	A	A		A				
Selektivní integrita zpráv	A	A		A				
Nepopiratelnost odeslání	A	A		A				A
Nepopiratelnost doručení	A	A		A				A

Tabulka 4.2 Přiřazení bezpečnostních mechanismů službám

4.1.3 Vztah ke kritériím CC

Kritéria CC se již snažila bezpečnostní funkce pro zabezpečení přenosu dat do sebe zahrnout. Způsob, kterým to bylo provedeno, je však poněkud komplikovaný. Funkce jsou rozptýleny po několika třídách a jejich identifikace je pracná. Například obě funkce nepopiratelnosti jsou ve třídě FCO (Komunikace), autentizace, důvěrnost a integrita uživatelských dat je ve třídě FDP (Ochrana uživatelských dat), další funkce jsou ukryty ve třídě FTP (Důvěryhodné cesty/kanály), FCS (Kryptografická podpora) a i některé další třídy obsahují bezpečnostní funkce, které mohou mít vztah k přenosu dat.

Lze tedy konstatovat, že bezpečnostní funkce pro přenos dat, zabudované do kritérií CC, nejsou přímou náhradou normy ISO 7498-2 a tato norma bude i nadále při hodnocení bezpečnosti potřeba.

Je třeba ještě říci, že standard ISO 7498-2 obsahuje pouze *bezpečnostní funkce*, tedy popis bezpečnostních opatření na vyšší úrovni. Pokud se hodnotí i bezpečnost samotných bezpečnostních mechanismů, je třeba použít další normy a standardy, včetně norem a standardů pro kryptografické mechanismy. Dneska už existuje poměrně velké množství takových norem a

standardů a jejich výčet nebo popis by se už vymykal obsahu této práce. Zájemci lze doporučit například publikaci [HS00a], která se právě touto problematikou zabývá.

4.2 Kritéria pro hodnocení kryptografických modulů

Kryptografické bezpečnostní mechanismy mohou být využity v nejrůznějších počítačových a telekomunikačních aplikacích (např. uchovávání dat, řízení přístupu a identifikace, datová, hlasová a obrazová komunikace) a v nejrůznějších prostředích (státní správa, bankovnictví a finančnictví, podnikání). Úroveň bezpečnosti kryptografického modulu musí být zvolena tak, aby zajišťovala dostatečnou ochranu dat v závislosti na bezpečnostních požadavcích, provozním prostředí a poskytovaných službách.

Podobně, jako se kritéria pro hodnocení bezpečnosti obvykle vyhýbají zabezpečení přenosu dat, vyhýbají se i definici požadavků na použité kryptografické mechanismy a kryptografické moduly. Specifikace těchto požadavků je ponechána na *národních standardech*.

Pokud konkrétní země nemá svůj vlastní standard, obvykle přebírá americký národní standard *Security Requirements for Cryptographic Modules, FIPS PUB 140-2* ([FIPS140]). Je to americký vládní standard pro implementace kryptografických modulů (hardwarových i softwarových), který vydala vládní organizace NIST (National Institute of Standards and Technology). Jeho cílem je specifikace požadavků, které musí splňovat návrh a implementace kryptografických produktů.

Standard specifikuje bezpečnostní požadavky, které musí splňovat kryptografické moduly, použité v bezpečnostních mechanismech, ochraňujících informace v počítačových a telekomunikačních informačních systémech. Zahrnuje implementace kryptografických modulů ve formě hardwarových komponent nebo modulů, softwarových programů nebo modulů, firmwarových modulů a v libovolné kombinaci předchozích případů.

4.2.1 Popis standardu

Standard definuje čtyři kvalitativní třídy bezpečnosti, které jsou nazvány Třída 1, Třída 2, Třída 3 Třída 4 (v originále Level 1, Level 2, Level 3 a Level 4) s postupně vzrůstajícími nároky na bezpečnost. Tyto úrovně pokrývají širokou škálu potenciálních aplikací a provozních prostředí, ve kterých je kryptografický modul nasazen. V návaznosti na to dokument *FIPS 140-2 Derived Test Requirements* [DTR] popisuje metody, které v této souvislosti jsou používány akreditovanými pracovišti při ověřování, zda konkrétní kryptografický modul splňuje požadavky normy FIPS 140-2. Dokument DTR obsahuje detailní procedury, analýzy a testy, které je v této souvislosti nezbytné provádět.

Bezpečnostní požadavky se vztahují zejména na oblasti návrhu a implementace kryptografického modulu, jako je základní návrh, dokumentace, rozhraní modulu, autorizované role a služby, fyzická bezpečnost, bezpečnost software, bezpečnost operačního systému, správa klíčů, použitý kryptografický algoritmus, elektromagnetická kompatibilita a autonomní testy.

4.2.2 Cíle bezpečnosti

Bezpečnostní požadavky specifikované v tomto standardu se vztahují k bezpečnému návrhu a implementaci kryptografického modulu. Požadavky jsou odvozeny z následujících obecných funkčních cílů činnosti kryptografického modulu. Cíle stanovují, že je nutno:

- Chránit samotný kryptografický modul před neautorizovaným přístupem nebo použitím.
- Zabránit neautorizovanému prozrazení neveřejných informací, uložených v kryptografickém modulu, včetně nezašifrovaných kryptografických klíčů a jiných parametrů, kritických z hlediska bezpečnosti.
- Zabránit neautorizované a neodhalené modifikaci kryptografického modulu, včetně neautorizovaného modifikování, nahrazení, vložení nebo zrušení kryptografických klíčů a jiných parametrů, kritických z hlediska bezpečnosti.
- Zajistit indikaci provozního stavu kryptografického modulu.
- Zajistit správnou činnost kryptografického modulu.
- Detekovat chyby v provozu kryptografického modulu a zabránit prozrazení citlivých informací v důsledku těchto chyb.

4.2.3 Bezpečnostní požadavky

Bezpečnostní požadavky, které musí splňovat kryptografický modul, jsou rozděleny do následujících oblastí:

- základní návrh a dokumentace
- rozhraní modulu - autorizované role a služby
- fyzická bezpečnost
- softwarová bezpečnost
- bezpečnost operačního systému
- správa klíčů - kryptografické algoritmy
- elektromagnetická kompatibilita a interference
- autonomní testování.

4.2.4 Definované třídy bezpečnosti modulu

Standard definuje následující čtyři třídy:

Třída 1

Třída 1 poskytuje nejnižší míru bezpečnosti. Tato třída specifikuje pouze základní bezpečnostní požadavky na kryptografický modul (například použití *standardizovaného nebo registrovaného* algoritmu). Pro kryptografický modul v této třídě nejsou požadovány žádné fyzické bezpečnostní mechanismy.

Příkladem hardwarových kryptografických modulů ve třídě 1 jsou zásuvné šifrovací karty do osobních počítačů a přenosné šifrovací adaptéry (např. PCMCIA karty), které slouží k distribuci klíčů nebo k samotnému šifrování.

Třída 1 také zahrnuje softwarové kryptografické mechanismy implementované na osobních počítačích (PC). Tyto implementace mohou být odpovídající v prostředích s nízkými požadavky na bezpečnost. Softwarová implementace kryptografických mechanismů na osobních počítačích je cenově mnohem přístupnější než hardwarové řešení. Zahrnutí softwarových kryptografických mechanismů na PC do třídy 1 dovoluje uživatelům, aby se vyhnuli situaci, kdy pro vysokou cenu hardwarového řešení raději neimplementují žádné bezpečnostní mechanismy.

Třída 2

Pro hardwarové kryptografické moduly třída 2 zavádí požadavky na fyzické zabezpečení kryptografického modulu pomocí obalu s evidencí fyzického útoku nebo uzamčení zámkem. Obal s evidencí fyzického útoku, jenž je dnes běžně dostupný, musí být nevratně porušen při každém pokusu o fyzický přístup ke kryptografickým klíčům nebo jiným kritickým parametrům. Zámky jsou umístěny na skříň nebo dvířka modulu za účelem zabránění fyzickému přístupu k modulu. Tyto bezpečnostní mechanismy jsou cenově dostupné pro širokou škálu aplikací.

Třída 2 musí zajistit autentizaci rolí, která zajišťuje, že modul autentizuje roli operátora a kontroluje jeho autorizaci k prováděným operacím s modulem.

Třída 2 rovněž dovoluje implementaci softwarových kryptografických modulů ve víceuživatelských operačních systémech s certifikací alespoň (E2, F-C2) podle kritérií ITSEC, tj. C2 podle kritérií TCSEC.

Třída 3

Třída 3 předepisuje pro hardwarové moduly zvýšenou míru fyzické bezpečnosti. Zatímco ve třídě 2 je požadován pouze zámek nebo obal s evidencí fyzického útoku, ve třídě 3 jsou požadovány bezpečnostní mechanismy, které zabrání útočníkovi v získání kritických parametrů umístěných uvnitř modulu. Například vícečipový kryptografický modul musí být umístěn v pevné schránce a musí být zajištěno, že při pokusu o otevření této schránky budou kritické parametry v modulu vynulovány. Kryptografické moduly s těmito fyzickými bezpečnostními mechanismy jsou dnes běžně komerčně dostupné.

Třída 3 musí zajistit autentizaci subjektů, jež je silnější než autentizace rolí, požadovaná ve třídě 2. Modul musí autentizovat identitu operátora a kontroluje jeho autorizaci k prováděným operacím s modulem.

Třída 3 obsahuje přísnější požadavky na vstup a výstup kritických parametrů. Datové brány, používané pro tyto parametry musí být fyzicky odděleny od ostatních datových bran. Pokud parametry jsou do modulu vkládány přímo (tak, že neprocházejí jinými částmi systému), mohou být vkládány v nezašifrované podobě. V opačném případě musí být vkládány v zašifrované podobě.

Třída 3 dovoluje implementaci softwarových kryptografických modulů ve víceuživatelských operačních systémech s certifikací alespoň (E3, F-B1) podle kritérií ITSEC, tj. B1 podle kritérií TCSEC. Systém musí poskytovat důvěryhodný kanál pro vkládání kritických

parametrů. Systém s certifikací (E3, F-B1) nebo lepší je požadován proto, aby bylo zajištěno oddělení kryptografického modulu od jiného nedůvěryhodného software, které běží v systému.

Třída 4

Moduly ve třídě 4 poskytují nejvyšší úroveň bezpečnosti. Ačkoli většina běžně komerčně dostupných kryptografických modulů nesplňuje požadavky této třídy, existují informační systémy, kde je tato nejvyšší úroveň bezpečnosti požadována. Pro hardwarové moduly požaduje třída 4 nepřekonatelnou fyzickou ochranu modulu. Zatímco fyzická bezpečnostní opatření modulů ve třídě 3 mohou být vysoce motivovaným a technicky vybaveným útočníkem překonána, třída 4 požaduje ochranu proti jakémukoli fyzickému útoku. Pokud se, například, útočník pokusí proříznout obal kryptografického modulu, pokus musí být detekován a kritické parametry musí být vymazány. Moduly ve třídě 4 jsou v zásadě určeny pro práci v prostředí bez jakékoli fyzické ochrany, kde útočník může do modulu jakkoli zasahovat.

Moduly ve třídě 4 musí být také chráněny proti prozrazení kritických parametrů v důsledku změny provozní teploty nebo provozních napětí mimo povolený rozsah. Modul musí být zabezpečen proti takovýmto změnám vnějšího prostředí nebo musí tyto změny detekovat a následně vymazat kritické parametry.

Třída 4 dovoluje implementaci softwarových kryptografických modulů ve víceuživatelských operačních systémech s certifikací alespoň (E4, F-B2) podle kritérií ITSEC, tj. B2 podle kritérií TCSEC.

4.2.5 Vztah ke kritériím CC

Podobně jako u přenosu dat se kritéria CC již snažila do sebe zahrnout i některé bezpečnostní funkce pro kryptografické moduly. Především se v nich objevila třída funkčních požadavků FCS (Kryptografická podpora), která se skládá ze dvou rodin: FCS-CKM Správa kryptografických klíčů a FCS-COP Kryptografické operace a která pokrývá většinu funkčních požadavků. V oblasti požadavků zaručitelnosti je však podpora kritérií CC pro kryptografické moduly nedostatečná. S pomocí CC je sice možno vytvořit profil ochrany pro kryptografický modul (například pro čipovou kartu), avšak je to značně komplikované a je k tomu třeba dodefinovat speciální funkční požadavky. Příkladem profilu ochrany, vytvořeného touto cestou, je *Smart Card Security User Group - Smart Card Protection Profile* ([SCSUGPP]).

Lze tedy konstatovat, že kritéria CC zvládají hodnocení kryptografických modulů pouze za cenu jistých komplikací a standard FIPS PUB 140-2 bude nadále používán.

4.3 Kritéria pro management bezpečnosti

Poslední oblastí, která je obvykle kritérii pro hodnocení bezpečnosti pokryta pouze částečně, je tzv. management informační bezpečnosti (zkráceně management bezpečnosti). Kritéria se managementu bezpečnosti obvykle věnují pouze okrajově, protože se předpokládá, že kritéria bezpečnosti slouží k hodnocení bezpečnosti *produktu* nebo *systému* informačních technologií. Management bezpečnosti má však mnohem širší záběr, protože zahrnuje bezpečnostní procesy celé *organizace*, ve které bude produkt nebo systém IT nasazen, a proto bývá hodnocen podle jiných norem nebo standardů.

Vhodným metodickým průvodcem problematikou managementu bezpečností IT je např. technická zpráva ISO/IEC TR 13335 "*Information technology – Guidelines for the Management of IT Technology*" ([TR13335]). Podle tohoto materiálu se bezpečnost IT použitých v organizaci dosahuje především plněním manažerských funkcí, souvisejících s bezpečností IT jako integrální součásti plnění globálního plánu správy organizace. Mezi takové manažerské funkce typicky patří:

- určení cílů, strategií a politik zabezpečení IT organizace
- určení požadavků na zabezpečení IT organizace
- identifikace a analýza hrozeb pro aktiva IT v rámci organizace
- identifikace a analýza rizik pro organizaci plynoucích z používání IT
- specifikace přiměřených bezpečnostních opatření eliminujících nebo snižujících rizika
- sledování implementace a provozu bezpečnostních opatření použitých pro účinnou ochranu informací a služeb IT v rámci organizace
- vyvinutí a zavedení programu zvyšování bezpečnostních znalostí a bezpečnostního povědomí
- detekování bezpečnostních incidentů a adekvátní reakce na ně.

Dokument TR 13335 je svým charakterem vhodný jako metodický materiál, avšak pro samotné hodnocení stavu managementu bezpečnosti by jeho použití bylo poněkud komplikované. Dokument je spíše technickou zprávou a nepředepisuje konkrétní a přesná kritéria, která je třeba posuzovat a kontrolovat. Pro tento účel je spíše vhodnější jiný dokument, a tím je norma ISO/IEC 17799.

4.3.1 Norma ISO/IEC 17799 (BS 7799)

Norma ISO/IEC 17799 (v české verzi ČSN ISO/IEC 17799, viz. [BS7799]) vznikla převzetím britského standardu BS 7799 a je velmi často nazývána svým původním názvem BS 7799, který je daleko více zažitý.

Původním určením standardu BS 7799 bylo poskytnout *návod* pro organizaci bezpečnostního managementu a zabezpečení informačních systémů běžných průmyslových podniků. Postupem času se význam tohoto standardu mírně posunul a dnes je tento standard běžně používán také pro hodnocení, zda management informační bezpečnosti určité instituce splňuje požadavky, definované standardem. Dnes se tento standard běžně používá pro tzv. certifikace managementu informační bezpečnosti institucí.

BS 7799 definuje deset hledisek, podle kterých je management informační bezpečnosti instituce kontrolován. Jde o následující hlediska:

Hledisko 1 - "Bezpečnostní politika"

Informační bezpečnost musí mít podporu managementu. Management musí odsouhlasit dokumenty o informační bezpečnosti, zajistit, aby s ním byli seznámeni všichni pracovníci a aby byla prováděna příslušná revize.

Hledisko 2 - "Organizační bezpečnost"

Cílem je ustavit řídící strukturu uvnitř subjektu, která by iniciovala a kontrolovala implementaci informační bezpečnosti. Výsledkem by mělo být zapojení a kooperace řídících pracovníků, uživatelů, administrátorů, vývojových pracovníků, auditorů a dalších specialistů do celého procesu.

Hledisko 3 - "Klasifikace a řízení aktiv"

Toto hledisko definuje nezbytnost zavedení klasifikace a řízení aktiv a přiřazení odpovědnosti za jednotlivá aktiva.

Hledisko 4 - "Personální bezpečnost"

Cílem opatření v oblasti personální bezpečnosti je snížit rizika vyplývající z lidských chyb, krádeže, podvodu nebo zneužití.

Hledisko 5 - "Fyzická bezpečnost a bezpečnost prostředí"

Cílem je zabránit neautorizovanému přístupu nebo poškození zařízení na zpracovávání informací. Zpracování informací by mělo být prováděno v bezpečných prostorách a k jejich ochraně by měly být zavedeny vhodné postupy.

Hledisko 6 - "Řízení komunikací a provozu"

Aby bylo zajištěno správné a bezpečné zpracování informací, musí být zavedeny příslušné postupy a přiřazeny odpovědnosti. Významné je zavedení a prosazení oddělení povinností, etapy plánování a akceptace u nových systémů, ochrana proti škodlivému softwaru, zajištění integrity a dostupnosti zpracování a komunikačních služeb. Do této oblasti patří také management sítí a zacházení s médii a zajištění bezpečnosti při výměně informací mezi jednotlivými subjekty.

Hledisko 7 - "Řízení přístupu"

K zabránění přístupu k informačním systémům je nezbytné zavést formální postupy pro přidělování přístupových práv, zejména u privilegovaných přístupových práv a zajistit, aby přijaté postupy pokrývaly všechna stadia životního cyklu přístupu uživatelů k datům.

Hledisko 8 - "Vývoj a údržba systému"

Cílem tohoto hlediska je zajistit, aby bezpečnost byla začleněna do systému již ve stadiu jeho návrhu a vývoje. Zabývá se také změnovým řízením, bezpečností systémových programů a správou kryptografických klíčů.

Hledisko 9 - "Řízení kontinuity činnosti systému"

Jedná se o opatření, která jsou nezbytná pro zajištění kontinuity činnosti daného subjektu, tj. ochrana informací a kritických procesů před následky selhání a jiných pohrom.

Hledisko 10 - "Zajištění shody"

Zde se jedná o postupy a opatření nezbytná k zajištění shody s právními požadavky, s vnitřními pravidly a předpisy subjektu, jako je bezpečnostní politika.

4.3.2 Vztah BS 7799 ke kritériím CC

Přestože kritéria CC obsahují funkční třídu *FMT: Správa bezpečnosti* a mohlo by se tedy zdát, že tím management informační bezpečnosti pokrývají, není tomu tak. Správa bezpečnosti ve třídě FMT se zabývá pouze správou dat, bezpečnostních atributů, funkcí a rolí uvnitř informačního systému a s managementem informační bezpečnosti organizace mají málo společného. Lze říci, že v této oblasti se kritéria CC téměř neuplatní (až na několik požadavků zaručitelnosti, jak uvidíme později) a hodnocení podle BS 7799 probíhá v podstatě paralelně s hodnocení podle CC. Jejich překryv je minimální.

5. Příklad hodnocení bezpečnosti podle CC

V této části práce popíšeme konkrétní nasazení některých dříve prezentovaných postupů na konkrétním příkladu informačního systému pro poskytování certifikačních služeb (ISCS). Tento příklad byl vybrán proto, že informační systémy poskytovatelů certifikačních služeb jsou první systémy v ČR, u kterých je požadováno hodnocení, hodnotitelnost nebo audit podle těchto kritérií. Je tedy i první oblastí, ve které jsou v ČR praktické zkušenosti s nasazením kritérií pro hodnocení bezpečnosti.

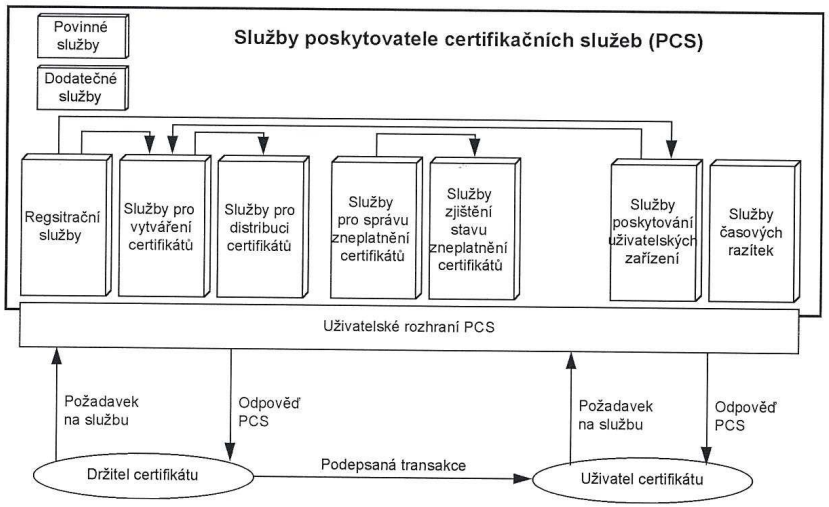
V této části práce nebude popisováno nasazení kritérií na jeden konkrétní systém, jde spíše o syntézu postupů, z nichž některé byly aplikovány u různých konkrétních systémů a některé ještě v době psaní práce aplikovány nebyly, ale je vypracována jejich, alespoň rámcová, metodika. V některých případech jsou zvažovány i různé varianty toho, jak lze úspěšně dospět k výsledku, požadovanému pro tento informační systém.

5.1 Motivace hodnocení

Jedním ze základních problémů kryptografie, který se projevuje v otevřených prostředích s velkým počtem navzájem neznámých partnerů, je otázka autenticity veřejných klíčů. Například v okamžiku ověřování elektronického podpisu si musí být ověřovatel jistý, že veřejný klíč, který používá k ověřování daného podpisu, je veřejným klíčem autora zprávy, tzn. potřebuje spolehlivou vazbu mezi klíčem a jménem. Bez dalších opatření by každý uživatel musel nějakým jiným způsobem provést ověření autenticity veřejného klíče každého partnera před tím, než by se na něj mohl spolehnout. Složitost tohoto problému může být zmenšena certifikací veřejných klíčů prostřednictvím někoho jiného, komu důvěřuje jak podepisující osoba, tak ověřující osoba. Tento prostředník, takzvaná certifikační autorita (CA), podepíše veřejný klíč uživatele a jeho jméno (a také další údaje jako například doba platnosti) svým vlastním soukromým klíčem. Tyto údaje, podepsané certifikační autoritou, se nazývají certifikát. Tento certifikát může být ověřen veřejným klíčem certifikační autority.

Vytváření certifikátů je však pouze jednou z činností, které provádí certifikační autorita. Obecně certifikační autorita (alternativní a obecnější název je Poskytovatel certifikačních služeb, PCS) může poskytovat několik služeb. Tyto služby se dělí na *povinné služby*, které musí implementovat každý PCS a *dodatečné služby*, které není nutno implementovat.

Povinné služby zahrnují registrační služby, služby pro vytváření certifikátů, služby pro distribuci certifikátů, služby pro správu zneplatnění certifikátů a služby zjištění stavu zneplatnění certifikátů. Dodatečné služby obsahují služby poskytování uživatelských zařízení a služby časových razítek. Struktura služeb PCS a jejich vazby jsou znázorněny na Obr. 5.1.



Obr. 5.1 Služby poskytovatele certifikačních služeb

PCS jsou instituce, které jsou na správné a bezpečné funkci jejich informačního systému životně závislé. Proto v České republice jsou stanoveny jisté podmínky pro PCS, vydávající kvalifikované certifikáty. Tyto podmínky stanovuje *Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č. 226/2002 Sb* ([ZOEP]) a *Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu* ([ZOEPV]). Mezi tyto podmínky patří:

- Existence dokumentů tzv. předpisové základny.
- Písemný posudek, že podle kontroly bezpečnostní shody, která byla provedena podle technické normy upravující oblast informační bezpečnosti, je používání ISCS v souladu s dokumenty předpisové základny. Jako technická norma, upravující oblast informační bezpečnosti, je akceptována norma ČSN ISO/IEC TR 13335 nebo ČSN ISO/IEC 17799.
- Výsledek hodnocení informačního systému pro certifikační služby (ISCS) na úroveň EAL4 podle normy ISO/IEC 15408 [I15408] .

Co se týče požadavku na úroveň EAL4 by bylo logické, aby PCS předložil hodnocení informačního systému pro certifikační služby na úroveň EAL4 podle normy ISO/IEC 15408, což jinými slovy znamená, že ISCS musí být *hodnocený* na úroveň EAL4. Vzhledem k tomu, že ne u všech systémů je v současné době k dispozici hodnocení podle této normy, dojde pravděpodobně k praxi, kdy bude vyžadován systém *hodnotitelný* na úroveň EAL4 (formulace požadavku zní: "*Používaný informační systém pro certifikační služby se považuje za bezpečný, pokud u dat, která zpracovává, je zajištěna důvěrnost, integrita, dostupnost a prokazatelnost jejich původu a pokud odpovídá požadavkům technické normy upravující oblast informační bezpečnosti. Touto technickou normou je: ČSN ISO/IEC 15408-3*"). V praxi

to znamená, že ISCS nemusí projít hodnocením ale musí být na toto hodnocení připraven. Musí tedy splňovat všechny požadavky na systém, připravený k hodnocení, včetně veškeré dokumentace. To, zda jsou tyto požadavky splněny, je možno spolehlivě zjistit vzhledem k velkému rozsahu dokumentace pouze nezávislým auditem.

V následujících kapitolách bychom si postupně ukázali možnosti, jak může PCS splnit požadované podmínky. Nejevíce prostoru budeme věnovat nejsložitějšímu problému, kterým je dosažení hodnotitelnosti ISCS na úroveň EAL4.

5.2 Obecné zásady pro hodnocení

Skladba jakéhokoli hodnocení bezpečnosti IS vychází ze tří možných pramenů:

a) z kritérií,

b) z metodologie,

c) z národních předpisů.

Kritéria představují měřítko, se kterým lze IT systém nebo IT produkt srovnávat při hodnocení, vývoji a pořizování. Kritéria definují, co se musí hodnotit. Metodologie definuje, jak by se mělo provádět hodnocení podle těchto kritérií. Národní předpisy určují organizační pravidla pro procesy hodnocení, certifikace, vývoje a akreditace laboratoří v pojmech rolí, procedur, práv a povinností.

5.2.1 Některé způsoby zkoumání

Většina kritérií nedoporučuje konkrétní techniky a nástroje pro zkoumání posuzovaného systému. Při zkoumání se mohou uplatnit národní předpisy a sortiment použitelných technik a nástrojů se trvale vyvíjí. Některé způsoby zkoumání jsou však všeobecně přijímány většinou kritérií a proto se o nich krátce zmíníme.

Neformální zkoumání

Úplně základní technikou je technika neformálního zkoumání dokumentů. Tuto techniku lze použít pro všechny jednodušší aktivity hodnotitele. Pro práci s neformálními nebo počítačově nečitelnými reprezentacemi prakticky neexistuje jiná alternativa této metody. Jsou s ní spojena jistá nebezpečí a je dobře počítat s tím, že:

a) Neformální zkoumání není vhodné provádět jedinou osobou po dlouhou dobu, poněvadž to snižuje kvalitu výsledků; pokud je to možné, měli by spolupracovat dva hodnotitelé současně.

b) Hodnotitelé provádějící neformální zkoumání musí vytvořit dostatečně dokumentované důkazy (např. mezivýsledky), které by umožnily usoudit, že práci provedli.

Analýza korespondence

Poněkud metodičtější technikou je analýza korespondence. Používá se pro analýzu konzistence dvou reprezentací. Tvoří ji dva kroky:

a) kontroluje se každá komponenta vyšší reprezentace, zda je její implementace v nižší vrstvě provedena správně;

b) kontroluje se, zda existence každé komponenty v nižší reprezentaci je oprávněná z hlediska vyšší reprezentace.

Jedná se opět o spíše manuální práci, o které platí to, co bylo řečeno výše. V některých případech lze s výhodou využít pro udržení korespondence mezi reprezentacemi automatizované systémy. Hodnotitelé musí být schopni prokázat, že při své analýze vzali do úvahy každou relevantní část posuzovaného systému.

Testování implementace

Jednotlivé komponenty systému je možno testovat vzhledem k jejich funkční specifikaci. Celý systém je pak možno testovat jako celek vzhledem k modelu bezpečnostní politiky. Je třeba počítat s tím, že testování komponenty nebo větší jednotky vzhledem k její specifikaci může ukázat pouze na chyby nebo odchylky od specifikace a nemůže potvrdit nepřítomnost chyb. Proto je potřeba na vyšších úrovních hodnocení doplnit testování potřebnými analýzami.

I když tato činnost spoléhá mnohem více než ostatní činnosti na automatizační prostředky, i ona používá částečně neformální zkoumání. Jestliže implementace zahrnuje zdrojové programy, lze pro posouzení kvality programu a pro nalezení konkrétních typů zranitelných míst použít prostředky pro statickou analýzu zdrojových programů. Jestliže implementace zahrnuje hardwarová schémata, lze pro jejich analýzu použít CAD prostředky vývojáře. Po hodnotitelích se požaduje kontrolovat, že testy pokrývají všechny bezpečnostní funkce systému.

Oponentní proces

Proces hodnocení zahrnuje nezanedbatelné množství neformální analýzy. Je důležité prokázat, že tato analýza byla provedena objektivně. Jedním ze způsobů, jak toho dosáhnout je kontrola každé práce hodnotitele jiným hodnotitelem.

Oponentního procesu by se měli zúčastnit alespoň následující role:

a) Vedoucí hodnocení, tj. ten, kdo je zodpovědný za technické vedení hodnocení.

b) Autor, tj. hodnotitel, který prováděl analýzu.

c) Moderátor, tj. ten, kdo je zodpovědný za nezávislé posouzení toho, že oponentura proběhla odpovídajícím způsobem.

Lze přizvat i jiné osoby, např. technické specialisty, představitele certifikačního orgánu a ostatní hodnotitele (zvláště tehdy, když autor a vedoucí hodnocení je jedna osoba).

5.3 Posouzení dokumentů předpisové základny

Požadavky na předpisovou základnu PCS jsou definovány zákonem č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů, v platném znění a vyhláškou č. 366/2001 Sb. Zákon a vyhláška požadují následující skladbu dokumentů:

- CP - certifikační politika CA.

- CPS - certifikační prováděcí směrnice CA.
- CBP - celková bezpečnostní politika poskytovatele certifikačních služeb.
- SBP - systémová bezpečnostní politika informačního systému pro certifikační služby.
- PKSPO - plán pro zvládání krizových situací a plánem obnovy řádné funkce informačního systému pro certifikační služby.
- ODF - odhad dostatečnosti finančních zdrojů poskytovatele certifikačních služeb a doklady o tom, že poskytovatel certifikačních služeb disponuje těmito finančními zdroji. Tento dokument však nemá nic společného s bezpečností informačních systémů, a proto se jím v dalším výkladu nebudeme zabývat.

Tvorba dokumentů předpisové základny

Zákon a vyhláška přímo nepředepisují obsah těchto dokumentů. Ze znění zákona a vyhlášky a ze znalosti oboru se však dají odvodit zásady pro obsah těchto dokumentů. Doporučuje se proto následující postup:

- ***CP a CPS - Certifikační politika a Certifikační prováděcí směrnice***

  Požadovaný obsah těchto dvou dokumentů je poměrně přesně specifikován standardem *RFC 2527: Certificate Policy and Certification Practices Framework* ([RFC 2527]). Tento standard dává návod, jakou strukturu by měly dokumenty CP a CPS mít. Vzhledem k tomu, že osnova obou dokumentů je dosti podobná, volí někteří autoři tu cestu, že nejdříve vytvoří dokument CPS (který je rozsáhlejší) a poté z něj vytvoří dokument CP vypuštěním některých kapitol a drobnou úpravou textu. Vzor osnovy pro CP a CPS v českém jazyce je v příloze A - "*Příklad osnovy CP a CPS*".

- ***CBP - Celková bezpečnostní politika***

  Celková bezpečnostní politika by měla být zpracována podle norem ČSN ISO/IEC TR 13335 nebo ČSN ISO/IEC 17799. CBP je základním dokumentem, který v organizaci upravuje informační bezpečnost. Je v organizaci každému známý (ČSN 13335-3, kap. 10.2; ČSN 17799, kap. 3), a měl by vytvářet předpoklady pro dosažení a udržení požadované úrovně bezpečnosti. Forma CBP není normami přesně specifikována. Je v nich pouze uveden doporučený seznam kapitol, které by CBP měla obsahovat. Například podle ČSN ISO/IEC TR 13335 by zde měly být zmíněny tyto oblasti:
  - Bezpečnostní požadavky na IT
  - Organizační infrastruktura a přiřazení zodpovědností
  - Bezpečnost vývoje a nákupu
  - Nařízení a procedury
  - Definice tříd pro klasifikaci informací
  - Strategie správy rizik
  - Havarijní plánování
  - Personální bezpečnost

- Školení a osvěta
- Právní problémy
- Správa outsourcingu
- Zvládání mimořádných událostí

Samotný způsob vypracování CBP je pro různé organizace rozdílný a závisí do značné míry na samotné organizaci. Více informací o bezpečnostních politikách nalezne čtenář například v publikaci [HS94a].

- ***SBP - systémová bezpečnostní politika***

  Pro SBP platí, stejně jako pro CBP, že by měla být zpracována podle norem ČSN ISO/IEC TR 13335 nebo ČSN ISO/IEC 17799. Tyto dokumenty však neposkytují žádný přesnější návod, jak by měla být SBP strukturována. V příloze B je proto uveden „Příklad struktury systémové bezpečnostní politiky". Více informací opět čtenář nalezne například v publikaci [HS94a].

- ***PKSPO - Plán pro zvládání krizových situací a plánem obnovy***

  Stejně jako CBP a SBP by měl být i PKSPO zpracován podle norem ČSN ISO/IEC TR 13335 nebo ČSN ISO/IEC 17799. Tyto dokumenty však nepředepisují strukturu ani obsah PKSPO. V příloze C je proto uveden „Příklad struktury PKSPO".

Hodnocení dokumentů předpisové základny

Zákon a vyhláška vyžadují pouze existenci dokumentů předpisové základny a nevyžadují jejich hodnocení. Avšak přesto, že auditování dokumentů předpisové základny není přímo předepsáno, doporučuje se, aby si PCS nechal tyto dokumenty auditovat. Audit se pak skládá z následujících kroků:

- ***Audit formální úplnosti předpisové základny***

  Cílem tohoto kroku je zjištění, zda auditovaná předpisová základna je formálně úplná z hlediska požadavků stanovených zákonem č. 227/2000 Sb. a vyhláškou č. 366/2001 Sb.

- ***Audit obsahové úplnosti předpisové základny***

  Cílem tohoto kroku je zjištění, zda dokumenty auditované předpisové základny obsahují informace požadované zákonem č. 227/2000 Sb. a vyhláškou č. 366/2001 Sb.

- ***Audit relevance obsahu předpisové základny***

  Cílem tohoto kroku je zjištění, zda obsah dokumentů auditované předpisové základny je relevantní požadavkům stanovených zákonem č. 227/2000 Sb. a vyhláškou č. 366/2001 Sb. a požadavkům na funkcionalitu a aplikační nasazení, stanovených samotným PCS.

- *Audit souladu předpisové základny s normami, předpisy a standardy*

  Cílem tohoto kroku je zjištění, zda je auditovaná předpisová základna v souladu se zákonem č. 227/2000 Sb. a s vyhláškou č. 366/2001 Sb. a dále pak, zda je v souladu s dalšími obecně platnými relevantními dokumenty.

5.4 Posouzení bezpečnostní shody

Dalším požadavkem na ISCS, je písemný posudek, že podle kontroly bezpečnostní shody, která byla provedena podle technické normy, upravující oblast informační bezpečnosti, je používání ISCS v souladu s dokumenty předpisové základny. Zde je klíčovým bodem technická norma, podle které je možno tento posudek vytvořit. Povoleny jsou dvě normy:

- ČSN ISO/IEC TR 13335
- ČSN ISO 17799

Jako standard pro audit je tedy možno použít obě normy podle volby auditora. Je však pravděpodobné, že více bude používána norma ISO 17799, protože je pro daný účel vhodnější. Navíc s jejím použitím při auditu je více zkušeností. Zde existuje několik metodologií pro provádění auditu, ze kterých je možno si vybrat. Typická metodologie se obvykle skládá z následujících kroků (podle principu ISO 17799 *Plan/Do/Check/Act*):

- Kontrola bezpečnostních dokumentů z pohledu konzistence, platnosti a relevance.
- Předběžný audit, ve kterém se identifikují hlavní nedostatky v auditované instituci.
- Příprava auditované instituce na samotný audit.
- Samotný externí audit shody skutečného stavu s bezpečnostní dokumentací a s požadavky ISO 17799.

Jelikož podrobnější popis některé z těchto už existujících metodologií by se příliš vzdaloval od záměru této práce, kterým jsou kritéria pro hodnocení bezpečnosti informačních systémů, nebudeme jej zde uvádět.

5.5 Hodnotitelnost ISCS podle EAL4

V souladu s požadavky na ISCS, je třeba zajistit, že ISCS bude splňovat míru zaručitelnosti EAL4 podle standardu CC (ISO/IEC 15408).

5.5.1 Rekapitulace požadavků

Úroveň EAL4 umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti odvozenou z průkazně používaného bezpečnostního inženýrství, založeného na dobrých komerčních vývojových praktikách, které, třebaže se požaduje vysoká přísnost, nepožadují mimořádně velké odborné znalosti, dovednosti a jiné zdroje.

Úroveň EAL4 je tudíž vhodná pro podmínky, ve kterých vývojář nebo uživatel požadují průměrnou až vysokou úroveň nezávisle zaručené bezpečnosti pro běžně prodávané zboží a jsou srozuměni s vynaložením dodatečných nákladů na specifické bezpečnostní konstruování.

Úroveň EAL4 především vyžaduje následující činnosti:

- Musí se provést analýza všech rozhraní a analýza podrobného (detailního) návrhu a implementace bezpečnostních funkcí. Požaduje se existence neformálního modelu bezpečnostní politiky produktu nebo systému IT. Provádí se nezávislá analýza zranitelnosti prokazující odolnost vůči útočníkům s malými možnostmi a schopnostmi.
- Správa konfigurace se analyzuje detailně, včetně jejích automatizačních prostředků.
- Úroveň EAL4 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL3, poněvadž se požaduje hodnocení detailnějšího popisu návrhu a implementace bezpečnostních funkcí a požadují se vylepšené mechanismy nebo procedury, které poskytují důvěru, že produkt nebo systém IT nebyl nějak narušen během vývoje nebo dodávky.

Hodnocení na úrovni EAL4 se proti úrovni EAL3 týká i automatizace konfiguračních postupů, pokrytí vlastní konfigurace, podpory správy konfigurace, detekce modifikace během dodávky, úplné sestavy vnějších rozhraní, implementace bezpečnostní funkcionality, detailního návrhu, neformálního modelu bezpečnostní politiky, dobře definovaných vývojových nástrojů, analýzy správnosti, analýzy zranitelnosti provedené vývojářem a provedení nezávislé analýzy zranitelných míst.

Úroveň EAL4 definuje následující třídy požadavků pro zaručitelnost:

Třída	Rodiny
ASE: Security target Bezpečnostního cíl	-
ACM: Configuration management Správa konfigurace	*Automatizace správy konfigurace (ACM_AUT.1)* *Schopnosti správy konfigurace (ACM_CAP.4)* *Rozsah správy konfigurace (ACM_SCP.2)*
ADO: Delivery and operation Dodávka a provoz	*Dodávka (ADO_DEL.2)* *Instalace, generování a spuštění (ADO_IGS.1)*
AGD: Guidance documents Dokumentace	*Administrátorská dokumentace (AGD_ADM.1)* *Uživatelská dokumentace (AGD_USR.1)*
ALC: Life cycle support Podpora životního cyklu	*Vývojová bezpečnost (ALC_DVS.1)* *Definice životního cyklu (ALC_LCD.1)* *Nástroje a techniky (ALC_TAT.1)*
AVA: Vulnerability assessment Analýza zranitelnosti	*Zneužití (AVA_MSU.2)* *Síla funkcí (AVA_SOF.1)* *Analýza zranitelnosti (AVA_VLA.2)*
ATE: Tests Testování	*Pokrytí (ATE_COV.2)* *Hloubka (ATE_DPT.1)* *Funkční testování (ATE_FUN.1)* *Nezávislé testování (ATE_IND.2)*
ADV: Development Vývoj	*Model Bezpečnostní politiky (ADV_SPM.1)* *Funkční specifikace (ADV_FSP.2)* *Specifikace architektury (ADV_HLD.2)* *Detailní specifikace (ADV_LLD.1)* *Implementace (ADV_IMP.1)* *Korespondence reprezentací (ADV_RCR.1).*

Obr. 5.1 Požadavky zaručitelnosti EAL4

5.5.2 Varianty řešení problému

V následujícím výkladu se budeme zabývat příkladem systému ISCS, který by měl být hodnotitelný podle kritérií CC na úroveň EAL4. Nejdříve je třeba si přesně definovat, co znamená pojem „hodnotitelný“. Zde je třeba vycházet z aktivit, které kritéria CC předepisují pro úspěšné hodnocení. Jde o následující tři aktivity:

1. *Aktivity vývojáře*. Jedná se o činnosti, které musí provádět vývojář při vývoji – např. musí mít zavedeny odpovídající postupy pro správu konfigurace, musí používat vhodné nástroje pro vývoj, musí mít zabezpečeno prostředí pro vývoj atd.
2. *Požadavky na obsah a prezentaci*. Pro úroveň EAL4 se jedná o vypracování cca 18 až 24 dokumentů, které jsou předloženy hodnotiteli.
3. *Aktivity hodnotitele*. Jedná se o činnosti, které provádí hodnotitel. Tyto činnosti jsou přesně předepsané a poměrně rozsáhlé (především se jedná o náročné posouzení korespondencí a o rozsáhlé testy). Pro úroveň EAL4 se obvykle předpokládá, že provedení těchto aktivit trvá podle rozsahu HP 6 až 15 měsíců.

Pokud jsou úspěšně provedeny aktivity 1 až 3, je systém *hodnocený*. Pokud jsou provedeny pouze aktivity 1 a 2, je systém *hodnotitelný*. V následujícím textu budeme tedy předpokládat provedení pouze aktivit vývojáře a kontrolu nebo hodnocení dokumentů podle požadavků na obsah a prezentaci.

Výklad budeme vést ze tří možných pohledů:

1. Z pohledu vývojáře se budeme zabývat formou a obsahem dokumentů, které musí vývojář vytvořit, aby dosáhl hodnotitelnosti systému na úroveň EAL4. Ve výkladu bude toto hledisko pod hlavičkou **Tvorba dokumentů**.
2. Opět z pohledu vývojáře se budeme zabývat formou a obsahem dokumentů, které musí vývojář vytvořit, pokud zakoupil některé komponenty systému, hodnocené na úroveň EAL3 a chce dosáhnout toho, aby celý systém dosáhl hodnotitelnosti na úroveň EAL4. Ve výkladu bude toto hledisko pod hlavičkou **Zvýšení úrovně z EAL3 na EAL4**.
3. Z pohledu nezávislého auditora nebo akreditačního orgánu se budeme zabývat posouzením, zda forma a obsah předložených dokumentů splňuje požadavky hodnotitelnosti na úroveň EAL4. Ve výkladu bude toto hledisko pod hlavičkou **Hodnocení dokumentů**.

Následující kapitoly jsou uspořádány podle jednotlivých tříd požadavků na zaručitelnost a vyjadřují se k dokumentům potřebným pro tyto třídy z výše uvedených tří pohledů.

5.5.3 Hodnocení PO/BC (APE, ASE)

Třídy Hodnocení profilu ochrany (APE) a Hodnocení bezpečnostního cíle (ASE) mají prokázat, že dokument Profil ochrany (PO) nebo Bezpečnostní cíl (BC) je úplný, konzistentní a technicky bezesporný.

V našem konkrétním případě systému ISCS nepředpokládáme, že by se provádělo vypracovávání nebo hodnocení profilu ochrany. Vždy bude použit již existující a hodnocený profil ochrany, typicky jde o standardní *Profil ochrany systému pro vydávání a správu certifikátů* („*Certificate Issuing and Management Components, Protection Profile*“, [PPCIMC]).

Dokument Bezpečnostní cíl však i v našem konkrétním případě vypracováván být může, i když to není příliš častá činnost. V případě, že by tomu tak bylo, je k dispozici poměrně podrobný návod, jak BC vypracovat. Jde o dokument ISO/IEC PDTR 15446: *Guide for the production of protection profiles and security targets* ([TR15446]). Zájemce o tuto problematiku proto odkazujeme na tento dokument.

5.5.4 Správa konfigurace (ACM)

Správa konfigurace (Configuration Management, CM) zajišťuje integritu HP během procesu jeho vývoje až do okamžiku distribuce. Zabraňuje také neoprávněné modifikaci HP a tím zajišťuje, že distribuovaná verze HP je totožná s verzí hodnocenou. Pro úroveň EAL4 zahrnuje tři rodiny:

Automatizace správy konfigurace (ACM_AUT.1)

Schopnosti správy konfigurace (ACM_CAP.4)

Rozsah správy konfigurace (ACM_SCP.2)

Tvorba dokumentů

Dokumentace správy konfigurace je obvykle obsažena ve třech dokumentech: „*Dokumentace správy konfigurace*“, „*Plán správy konfigurace*“ a „*Akceptační plán*“.

Dokument „*Dokumentace správy konfigurace*“ popisuje prostředky a postupy, které poskytuje použitý systém pro správu konfigurace.

Dokument „*Akceptační plán*“ popisuje procedury, použité pro zabudování modifikovaných nebo nově vytvořených komponent do HP.

Dokument „*Plán správy konfigurace*“ by měl obsahovat alespoň:

- Seznam akcí, které jsou sledovány systémem správy konfigurace.
- Role a zodpovědnosti zúčastněných osob.
- Procedury, které zajišťují, že pouze oprávněné osoby mohou měnit komponenty HP.
- Procedury, které zajišťují, že nemohou vzniknout problémy při současné změně HP více osobami.
- Popis průkazných záznamů, generovaných jako výsledek prováděné změn.
- Popis tvorby označení verzí HP.

Hodnocení dokumentů

Hodnocení dokumentů se provádí neformálním zkoumáním a oponováním. Existují-li různé možnosti konfigurace, musí být v dokumentech popsán vliv, který mají jednotlivé konfigurace na bezpečnost. Musí být popsány procedury pro generování systému. Každá volba generování a změna v generování HP musí být provedena tak, že je kdykoliv možno znovu přesně rekonstruovat, jak a kdy byl HP generován.

Konfigurační seznam musí vyjmenovat všechny základní komponenty, ze kterých je postaven HP. Daný HP, jeho základní komponenty a veškerá dokumentace, včetně manuálů, zdrojových textů a hardwarových schémat, musí mít jednotný identifikátor. Užití tohoto jednotného identifikátoru je povinné ve všech odkazech. Systém řízení konfigurace musí potvrdit, že HP je hodnocen podle poskytnuté dokumentace a že jsou možné pouze autorizované změny.

Na úrovni EAL4 je vývojář povinen používat automatizované systémy řízení konfigurace. Systémy řízení konfigurace musí zajistit, že ve všech fázích životního cyklu HP existuje jasná, úplná a přesná reprezentace HP. Tato reprezentace musí odrážet všechny změny konfigurace.

6. Doporučený způsob provádění kontroly integrity systému souborů.
7. Pravidla pro efektivní využívání bezpečnostních mechanismů systému. Pravidla pro bezpečné generování nového systému.
8. Seznam všech parametrů se vztahem k bezpečnosti, které může měnit správce systému.
9. Doporučení pro nastavení parametrů systému hesel, systému vzdáleného přístupu, doporučení pro tvorbu havarijních plánů.
10. Seznam obvyklých způsobů útoku na systém a potenciálních hrozeb spolu s návodem, jak je detekovat a zabránit jim.
11. Popis procedur, které jsou nezbytné pro bezpečný start a inicializaci systému.
12. Popis procedur, které jsou potřebné pro bezpečné zotavení systému pro chybě nebo havárii.
13. Popis procedur pro zálohování a obnovu dat.

Hodnocení dokumentů

Hodnocení dokumentů se provádí neformálním zkoumáním a oponováním. Hodnotitelé se seznamují s provozní dokumentací a ujišťují se, že zde uvedené informace jsou přesné a dostatečné pro bezpečnou konfiguraci a bezpečné provozování systému.

Zvýšení úrovně z EAL3 na EAL4

Při zvýšení úrovně z EAL3 na EAL4 nedochází k žádné změně, protože požadavky v této třídě jsou pro EAL3 a EAL4 stejné.

5.5.7 Podpora životního cyklu

Tato třída definuje požadavky na zajištění zaručitelnosti prostřednictvím modelu životního cyklu během vývoje. V jiných kritériích jsou tyto požadavky obvykle nazývány „požadavky na bezpečnost vývojového prostředí". Obsahuje tři rodiny: *Vývojová bezpečnost (ALC_DVS.1)*, *Definice životního cyklu (ALC_LCD.1)* a *Nástroje a techniky (ALC_TAT.1)*.

Tvorba dokumentů

Dokumentace pro tuto třídu bývá obvykle zpracována ve třech samostatných dokumentech. Dokument *Vývojová bezpečnost* je v podstatě systémovou bezpečnostní politikou vývojáře a je psán podle stejných zásad jako systémová bezpečnostní politika.

Dokument *Definice životního cyklu* obsahuje popis procesů projektového řízení, které definují životní cyklus vyvíjeného HP. Tento popis bývá obvykle převzat ze vhodné dokumentace použitého systému řízení projektu.

Dokument *Nástroje a techniky* obsahuje detailní popis použitých softwarových a hardwarových nástrojů, včetně jejich specifikace a konfigurace.

Hodnocení dokumentů

Dokument o bezpečnosti vývojového prostředí musí mimo jiné stanovit plánovanou bezpečnost integrity HP a důvěrnosti připojených dokumentů. Musí být popsána fyzická, procedurální, personální a další bezpečnostní opatření, která využívá vývojář.

Hodnotitel zkoumá, zda dokumentace obsahuje informace o řízení konfigurace, programovacích jazycích a obecně o procedurách, metodách, prostředcích a standardech, které byly použity během vývoje HP.

Každý programovací jazyk určený pro implementaci musí být dobře definován, například podle normy ISO. Každá volba programovacího jazyka, závislá na implementaci, musí být dokumentována. Definice programovacích jazyků musí jednoznačně určovat význam všech příkazů užitých ve zdrojových textech.

Zvýšení úrovně z EAL3 na EAL4

Zvýšení úrovně z EAL3 na EAL4 je v této třídě komplikované. Na úrovni EAL4 se objevují dvě nové rodiny – Definice životního cyklu a Nástroje a techniky, které na úrovni EAL3 nebyly vyžadovány a které je potřeba pokrýt odpovídajícími dokumenty.

5.5.8 Analýza zranitelnosti

Tato třída definuje požadavky směřující k identifikaci využitelných zranitelných míst v HP. Její rodina *Zneužití (AVA_MSU.2)* zajišťuje, že uživatel nebo administrátor je na základě uživatelské (administrátorské) dokumentace schopen detekovat, že systém se nachází ve stavu, který není bezpečný. Rodina *Síla funkcí (AVA_SOF.1)* vyžaduje, aby vývojář provedl analýzu síly bezpečnostních funkcí. Rodina *Analýza zranitelnosti (AVA_VLA.2)* vyžaduje, aby vývojář identifikoval zranitelná místa HP a ukázal, že tato zranitelná místa nejsou využitelná útočníkem.

Tvorba dokumentů

Pro rodinu *Zneužití* není třeba vypracovávat žádný dodatečný dokument. Pro zbylé dvě rodiny je třeba vypracovat dokumenty *Analýza síly funkcí* a *Analýza zranitelnosti*.

Kritéria CC nepředepisují žádnou kategorizaci síly bezpečnostních funkcí. Lze využít kategorizace z kritérií ITSEC, ale rozdělení síly mechanismů podle kritérií ITSEC na základní, střední a vysokou jsou pro vyjádření potřeb uživatelů velmi hrubé. Definice neposkytují detailní prostředky pro posuzování během hodnocení.

Pokud hledáme objektivnější měřítko, je třeba při kategorizaci síly bezpečnostních mechanismů vzít v úvahu znalosti, příležitost a prostředky útočníka:

a) Znalosti vyjadřují míru vědění, kterou musí mít osoba, aby byla schopna zaútočit na HP. Začátečník je ten, kdo nemá žádné zvláštní znalosti. Zkušený je seznámený s interní činností HP. Expert je seznámený s principy a algoritmy, použitými v HP.

b) Prostředky vyjadřují objem prostředků, které musí útočník vynaložit k úspěšnému útoku na systém. Hodnotitelé zpravidla uvažují dva typy prostředků: čas a vybavení. Čas je doba, kterou útočník potřebuje na provedení útoku a nezahrnuje se do ní doba studia. Vybavení zahrnuje počítače, elektronická zařízení, technické prostředky a programy.

c) Příležitost zahrnuje faktory, které obecně není schopen útočník ovlivnit, jako je požadavek na asistenci jiné osoby (komplot), pravděpodobnost výskytu jisté speciální kombinace okolností (šance) a pravděpodobnost a následky odhalení útočníka (detekce).

Podrobnější popis způsobu určení síly mechanismů na základě těchto vstupních údajů nalezne čtenář v publikaci ([ITSEM]).

Analýza zranitelnosti vychází z konceptu, že vývojář HP odhaduje způsoby vedení útoku proti HP a podle toho vybírá protiopatření. Hodnotitelé vycházejí z analýzy vývojáře a aby určili všechny způsoby, kterými lze narušit bezpečnostní cíle, nezávisle zkoumají HP z pohledu útočníka.

Hodnocení dokumentů

Hlavní technikou pro tuto činnost je neformální zkoumání uživatelské a administrátorské dokumentace, Analýzy síly mechanismů a Analýzy zranitelnosti .

Analýza hodnotitele by si měla všímat následujících generických metod, které mohou být použity pro využití zranitelných míst:

a) změna předdefinované posloupnosti aktivace komponent;

b) spuštění doplněné komponenty;

c) porušení řazení pomocí přerušení nebo pomocí plánovacích funkcí;

d) přímé a nepřímé čtení, zápis a modifikace vnitřních dat;

e) spuštění dat jako program;

f) použití komponenty v nepředpokládaném kontextu nebo pro nepředpokládaný účel;

g) generování neočekávaného vstupu komponenty;

h) aktivace zotavení po chybě;

i) použití implementačního detailu zavedeného v nižší reprezentaci;

j) porušení souběžnosti;

k) použití interference mezi komponentami neviditelnými na vyšší úrovni abstrakce;

l) zneplatnění předpokladů a vlastností, na kterých závisí komponenty na nižší úrovni;

m) využití prodlev mezi okamžiky kontroly a použití.

Zvýšení úrovně z EAL3 na EAL4

Zvýšení úrovně z EAL3 na EAL4 v této třídě není příliš obtížné. Nevzniká požadavek na žádný nový dokument, pouze jsou některé požadavky zpřísněny.

5.6.9 Testování

Jednotlivé komponenty systému musí být testovány vzhledem k jejich funkční specifikaci a modelu architektury. Celý systém musí být potom kontrolován a testován jako celek vzhledem k modelu bezpečnostní politiky. Je třeba počítat s tím, že testování komponenty nebo větší jednotky vzhledem k její specifikaci může ukázat pouze na chyby nebo odchylky od specifikace

a nemůže potvrdit nepřítomnost chyb. Proto je potřeba na vyšších úrovních hodnocení doplnit testování potřebnými analýzami.

Tato třída se skládá ze čtyř rodin: Rodina *Pokrytí (ATE_COV.2)* se zabývá požadavky na úplnost testů, rodina *Hloubka (ATE_DPT.1)* se zabývá detailností testů a rodina *Funkční testování (ATE_FUN.1)* slouží k definování sady testů, které zajišťují, že HP splňuje alespoň požadavky na vybrané funkční komponenty. Rodina *Nezávislé testování (ATE_IND.2)* předepisuje provedení části testů nezávislým subjektem.

Tvorba dokumentů

Třída testování je zpracována ve třech dokumentech – *Analýza pokrytí testů*, *Analýza hloubky testů* a *Testovací dokumentace*. Rodina Nezávislé testování nevyžaduje žádný samostatný dokument.

Hodnocení dokumentů

Hlavní technikou pro tuto činnost je neformální zkoumání dokumentace. Hodnotitelé by měli zkontrolovat, zda testy pokrývají všechny funkce prosazující bezpečnost vyjmenované ve specifikaci bezpečnosti. Hodnotitelé minimálně musí kontrolovat, že pro každý testovaný výrok ve specifikaci bezpečnosti bude definován alespoň jeden test, který prokáže jeho splnění. Užitečnou informaci pro tento účel může poskytnut vyjádření vývojáře, proč rozsah pokrytí testy je dostatečný.

Zvýšení úrovně z EAL3 na EAL4

Při zvýšení úrovně z EAL3 na EAL4 nedochází k žádné změně, protože požadavky v této třídě jsou pro EAL3 a EAL4 stejné.

5.5.10 Vývojový proces

Základním požadavkem v oblasti vývojový proces je existence specifikací bezpečnosti na několika úrovních. Specifikace bezpečnosti přesně popisuje důležité aspekty bezpečnosti zkoumaného systému a jejich vztah k chování systému. Prvotním účelem specifikace bezpečnosti je poskytnout nezbytnou úroveň porozumění, nutnou pro úspěšnou implementaci klíčových bezpečnostních požadavků. Důležitou úlohu při určování obsahu specifikace bezpečnosti hraje *bezpečnostní politika*. Proto je pro úspěšný vývoj specifikace bezpečnosti nutné, aby existovala úplná a konzistentní bezpečnostní politika. Pokud vytváříme formální specifikaci bezpečnosti, musí být vývoj této specifikace založen na vhodném matematickém aparátu pro popis a analýzu této specifikace.

Kritéria CC předpokládají, že se proces vývoje skládá z pěti fází, ve kterých se vytváří pět úrovní specifikace:

Fáze 1 – Model bezpečnostní politiky

Bezpečnostní politika specifikuje množinu zákonů, pravidel a praktik, které určují, jakým způsobem jsou organizovány, chráněny a distribuovány uvnitř daného systému citlivé informace a jiné zdroje. Musí určovat bezpečnostní cíle systému a jeho možné hrozby.

Bezpečnostní politika musí pokrýt všechny aspekty bezpečnosti hodnoceného systému, včetně souvisejících fyzických, personálních a procedurálních bezpečnostních opatření.

Fáze 2 – Funkční specifikace

Bezpečnostní cíle musí být plněny konkrétními bezpečnostními funkcemi a pomocí fyzických, personálních nebo procedurálních postupů, které se vztahují k systému.

Funkční specifikace musí obsahovat specifikaci bezpečnostních funkcí, které bude systém obsahovat. Tyto funkce mohou být specifikovány explicitně nebo odkazem na jednu z několika předem definovaných tříd funkčnosti, případně odkazem na přijatý standard, který definuje bezpečnostní funkčnost. Tyto funkce musí být vždycky specifikovány alespoň neformálním způsobem pomocí přirozeného jazyka. Na vyšších úrovních hodnocení musí být navíc specifikovány v poloformální nebo formální podobě.

Fáze 3 - Specifikace architektury

Tato fáze vývojového procesu zahrnuje všechny definice nejvyšší úrovně a návrh IS. Má formu popisné specifikace na vysoké úrovni a identifikuje základní strukturu IS, jeho externí rozhraní a dělení na nejdůležitější hardwarové a softwarové komponenty. Specifikace rozlišuje mezi tím, co IS dělá a jak to dělá. Je důležité, aby návrh architektury zachovával jasné a efektivní dělení na bezpečnostní komponenty a ostatní komponenty. Dobrý návrh umožňuje soustředit pozornost na omezené oblasti IS, které přispívají k bezpečnosti.

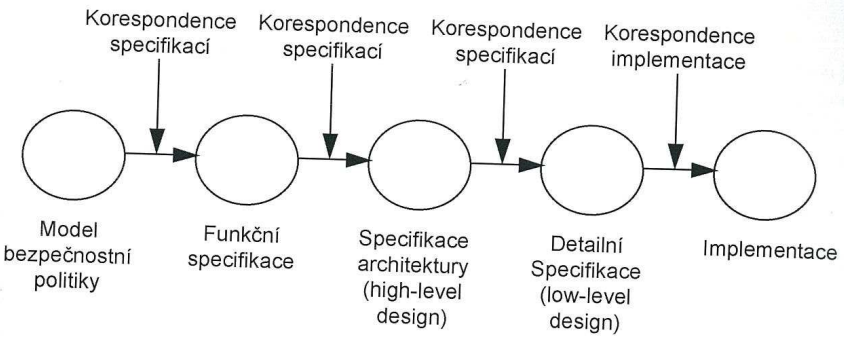
Fáze 4 - Detailní specifikace

Tato fáze vývojového procesu pokrývá zjemňování návrhu architektury do takových detailů, že může být využit jako základ pro programování nebo konstrukci hardware. Znamená to, že tato fáze zahrnuje všechna stadia návrhu a specifikace na nižší úrovni abstrakce. Je důležité, aby s podrobnější specifikací a menší abstraktností specifikace se transformace do jednotlivých komponent uskutečňovala způsobem, který zachovává smysl popisu na vyšší úrovni.

Fáze 5 - Implementace

Tato fáze vývojového procesu pokrývá implementaci detailního návrhu IS do podoby konkrétního hardware nebo software. Každá základní komponenta je nejprve naprogramována nebo postavena na základě specifikace. Jednotlivé základní komponenty jsou potom kontrolovány a testovány vzhledem k jejich specifikaci. Jednotlivé základní komponenty jsou dále vzájemně integrovány do podoby kompletního IS. Celý IS musí být potom kontrolován a testován jako celek vzhledem k specifikaci bezpečnosti.

Mezi těmito úrovněmi musí být vztah *korespondence* - viz. Obr. 5.2.



Obr. 5.2 Jednotlivé specifikace a jejich korespondence

Specifikace musí být zadány takovým způsobem, že vztahy mezi nimi jsou jasné a je-li specifikacemi zmiňován stejný bod, pak je tento bod vyhodnocován konzistentně. Paralelní specifikace mohou tvořit buď samostatné dokumenty, nebo mohou být začleněny do jednoho dokumentu.

Specifikace mohou být vypracovány způsoben neformálním, poloformálním nebo formálním (detailní definice způsobů realizace specifikací je uvedena v příloze D – „*Realizace specifikací*").

Výše definovaným fázím vývoje odpovídá prvních pět rodin třídy Vývojový proces. Jde o rodiny *Model Bezpečnostní politiky (ADV_SPM.1), Funkční specifikace (ADV_FSP.2), Specifikace architektury (ADV_HLD.2), Detailní specifikace (ADV_LLD.1) a Implementace (ADV_IMP.1)*. Vztah mezi těmito specifikacemi řeší poslední rodina *Korespondence reprezentací (ADV_RCR.1)*.

Pro úroveň EAL4 mohou být všechny tyto specifikace neformální.

Tvorba dokumentů

Jednotlivé specifikace jsou obvykle zpracovány v samostatných dokumentech, jejichž názvy zpravidla odpovídají použitým názvům specifikací. Struktura těchto dokumentů je velmi individuální a je silně ovlivněna vývojovými prostředky, které vývojář používá. Podkladem pro rodinu *Implementace* není textový dokument, ale vybraná podmnožina implementace HP. V případě softwarového HP jde tedy o podmnožinu zdrojových textů, v případě hardwarového HP o podmnožinu schémat. Tato podmnožina musí však zcela pokrývat bezpečnostní funkce HP.

Korespondence reprezentací bývá buď v jediném společném dokumentu nebo ve čtyřech samostatných dokumentech. Struktura korespondence je opět individuální a závislá na vývojových prostředcích.

Hodnocení dokumentů

Hlavní technikou této činnosti je neformální zkoumání specifikací. První částí tohoto procesu je hodnocení každé specifikace samostatně. Zde se kontroluje zejména úplnost a platnost dokumentů.

Druhou částí je zkoumání korespondence mezi specifikacemi. Hodnotitel kontroluje, zda jsou bezpečnostní funkce uvedené ve specifikaci bezpečnosti při přechodu od vyšší úrovně specifikace k nižší úrovni specifikace upřesňovány správně. Základní technikou hodnocení je tedy sledování každé bezpečnostní funkce v různých reprezentacích HP, a to až do úrovně implementace..

Zvýšení úrovně z EAL3 na EAL4

Zvýšení úrovně z EAL3 na EAL4 je v této třídě opět komplikované. Na úrovni EAL4 se vyskytují tři nové rodiny – *Model Bezpečnostní politiky, Detailní specifikace (ADV_LLD.1) a Implementace (ADV_IMP.1)*. Tyto rodiny na úrovni EAL3 nebyly vyžadovány a je potřeba pro ně vytvořit odpovídající podklady, což může být bez intenzivní spolupráce s vývojářem obtížné, ne-li nemožné.

5.6 Závěrečné poznámky

Obsahem této části práce byla ilustrace použití kritérií pro hodnocení bezpečnosti informačních systémů na konkrétním příkladě informačního systému pro poskytování certifikačních služeb. Požadavky byly převzaty z reálných požadavků, plynoucích z české legislativy. Z toho vyplývala i možnost v oblasti hodnocení ISCS na úroveň EAL4 nevyžadovat *hodnocený* systém, ale *hodnotitelný* systém. Z rozboru potřebných aktivit plynou následující závěry:

Z pohledu akreditačního orgánu nebo nezávislého auditora je hodnotitelnost systému ISCS na úroveň EAL4 záležitost poměrně dobře zvládnutelná. Posouzení předložených dokumentů je sice náročné na odborné znalosti, ale tento proces v sobě neskrývá žádné velké záludnosti.

Z pohledu vývojáře, který systém ISCS skládá z komponent, které jsou již hodnoceny na úroveň EAL4, jde o úkol opět poměrně dobře zvládnutelný. Pokud předpokládáme, že vývojář dopracovává pouze menší část systému, může do značné míry využít dokumentaci, získanou od vývojáře jednotlivých hodnocených komponent.

Z pohledu vývojáře, který systém ISCS celý vyvíjí, se jedná o úkol dobře zvládnutelný, ale značně nákladný a náročný na kapacity. Počet dokumentů, které musí vytvořit je značný a ke tvorbě těchto dokumentů jsou zapotřebí odborníci se specializovanými znalostmi.

Z pohledu vývojáře, který systém ISCS skládá z komponent, které jsou již hodnoceny na úroveň EAL3, jde o úkol velmi obtížný, snad i téměř nesplnitelný. Rozdíly mezi požadavky EAL3 a EAL4 jsou v některých třídách značné a rozdílové dokumenty prakticky není možno vytvořit bez velmi těsné spolupráce s vývojářem původních komponent.

6. Závěr

Závěrem bych chtěl shrnout přínosy prezentovaných výsledků původního autorova výzkumu a vývoje v oblasti kritérií hodnocení bezpečnosti informačních systémů, metodiky jejich hodnocení, aplikaci hodnocení bezpečnosti ve státní správě a ve vzdělávacím procesu.

Vědecko-výzkumný přínos

Cílem předkládané habilitační práce bylo popsat možnosti a postupy při aplikaci moderních kritérií pro hodnocení bezpečnosti některých typů informačních systémů v prostředí ČR. Byl uveden jednak základní přehled nejznámějších kritérií, včetně historických a technických souvislostí mezi nimi. Přehled byl také rozšířen o standardy a kritéria, která svým původním účelem nebyla určena přímo pro hodnocení bezpečnosti IS, ale při hodnocení bezpečnosti se používají. Vlastním přínosem autora je především analýza a popis vztahu mezi jednotlivými kritérii a standardy, definice jejich vztahu a eventuelně popis jejich zastupitelnosti.

V druhé části práce bylo popsáno nasazení některých prezentovaných postupů na třídu informačních systémů pro poskytování certifikačních služeb. Nebylo popisováno nasazení kritérií na jeden konkrétní systém, ale jde hlavně o syntézu postupů, z nichž většina byla aplikována u několika konkrétních systémů a některé ještě v době psaní práce aplikovány nebyly, ale je vypracována jejich, alespoň rámcová, metodika. Příklad byl zvolen úmyslně tak, aby bylo možno prezentovat postupy při posuzování bezpečnosti rozsáhlého systému, pro jehož posouzení který je třeba použít kombinaci kritérií a standardů.

Prezentované výsledky výzkumné činnosti autora vznikly v rámci grantů GAČR, FRVŠ, NBÚ a v rámci spolupráce s některými institucemi státní správy.

Úspěšné uplatnění výsledků v praxi a ve státní správě

Úvodní část práce má částečně přehledový charakter, avšak ani v této části nejde o pouhý kompilát z jiných publikací, ale o výsledek dlouholetého aktivního působení v této oblasti, neboť autor se aktivně účastnil zavádění různých standardů bezpečnosti do praxe v ČR, především v oblasti státní správy. V době, kdy perspektivními kritérii pro Českou republiku byla kritéria ITSEC, byl autor jedním ze dvou překladatelů dokumentu [ITSEC] a [ITSEM] do českého jazyka a spoluautorem publikace [HS94a] *„Bezpečnost informačních systémů - příručka pro projektanty a správce informačních systémů ve státní správě ČR"*, která byla rozsáhlým metodickým materiálem ke kritériím ITSEC a která byla využívána ve státní správě. Později se autor stal členem Technické normalizační komise "Informační technologie" Českého normalizačního institutu a v pracovní skupině SC27 se účastnil zavádění kritérií CC do našeho systému státních norem, kde jsou tato kritéria pod názvem ČSN ISO/IEC 15408. Autor je rovněž spoluautorem knihy [HS00a] "*Bezpečnost informačních systémů*", která má hlavní uplatnění opět ve státní správě a je zatím nejrozsáhlejší publikací v ČR, věnující se standardům bezpečnosti informačních systémů.

V oblasti poskytovatelů certifikačních služeb a elektronického podpisu se autor opět aktivně účastnil dění v ČR, neboť byl v letech 2001 až 2003 členem odborné pracovní skupiny ÚOOÚ (Úřad pro ochranu osobních údajů) pro elektronický podpis a spolupracoval při vytváření předpisů pro akreditaci poskytovatelů certifikačních služeb a metodik hodnocení bezpečnosti jejich systémů.

Uplatnění výsledků ve vzdělávacím procesu

Autor v současnosti vyučuje na FIT VUT bezpečnost informačních systémů a je připraveno a schváleno rozšíření této výuky na více předmětů v nově koncipovaném magisterském studijním programu. Autor také přednáší bezpečnost informačních systémů na několika nepravidelných kurzech. Důležitou částí uplatnění výsledků ve vyučovacím procesu je spolupráce se studenty, kteří se účastní řešení projektů z této oblasti v rámci ročníkových a diplomových prací.

Směr dalšího výzkumu

Mohlo by se zdát, že vědní disciplína hodnocení bezpečnosti informačních systémů zde existuje již dlouhou dobu, bylo v něm vykonáno hodně práce a v současnosti již není co zkoumat a postačuje aplikovat dříve objevené postupy do praxe. Ve skutečnosti tato vědní disciplína na tom zdaleka není tak optimisticky. I přes poměrně velké množství kritérií a metodologií, které byly vyvinuty, je v současné době počet systémů, které prošly jakýmkoli hodnocením neúnosně malý. Například v České republice zatím žádný, zde vyvinutý systém, neprošel v plné míře hodnocením podle některých kritérií bezpečnosti IS, jako je TCSEC, ITSEC nebo CC. Několik málo systémů je vydáváno za hodnotitelné, ale u části z nich je možno i tuto "hodnotitelnost" úspěšně zpochybnit. Hlavním problémem, který je stále nevyřešen, je časová náročnost a pracnost hodnocení prováděného podle současných metodologií.

Jedním z významných dnešních úkolů vědeckého výzkumu, zabývajícího se hodnocením bezpečnosti informačních systémů, je proto hledání efektivních a pokud možno automatizovaných metod hodnocení. Dnes je už zřejmé, že to nebude možné bez využití moderních poznatků z jiných oborů. Nejbližším kandidátem pro tuto spolupráci je softwarové inženýrství, které musí dát procesu hodnocení podklady o jednotlivých fázích vývoje informačního systému ve strojově zpracovatelné podobě. Dalšími kandidáty jsou formální metody a umělá inteligence, které musí poskytnout systémy pro efektivní posouzení korespondence jednotlivých fází vývoje. V budoucnu nás čeká také spolupráce se sociálními vědami, které by měly poskytnout podporu pro analýzu netechnických částí informačních systémů, jako jsou procesy v organizacích nebo chování jednotlivců a skupin.

Tyto cíle sleduje i další autorův výzkum, především v oblasti systémů pro automatizovanou analýzu rizik informačních systémů. Ačkoli v této oblasti výzkumu zatím ještě nelze nabídnout ucelené a prakticky použitelné výsledky, hodně práce již bylo vykonáno (viz. např. publikace [HRA97a], [HRA97b], [HRA98a], [HRA99a], [HPR00], prezentované na mezinárodních konferencích).

7. Literatura

7.1 Seznam použitých publikací

[AAL93] Abrams, M. D., Amoroso, E. G., LaPadula, L. J., Lunt, T. F., Williams, J. G.: Report of an integrity research study group, Computers & Security 12, Elsevier Science Ltd. 1993, p. 679–689

[AMO94] Amoroso, E. G.: Fundamentals of Computer Security Technology, ISBN 13–305541–8, Prentice Hall 1994

[AND85] Anderson, J. P.: A Unification of Computer and Network Security Concepts, Security and Privacy Volume 2, Proceedings of the 6th, 7th and 8th Symposia 1985–1987, IEEE 1990, p. 77–87

[AND94] RJ Anderson, ``Why Cryptosystems Fail", in Communications of the ACM v 37 no 11 (Nov 94) pp 32-40

[AND96] RJ Anderson, MG Kuhn, ``Tamper Resistance --- a Cautionary Note", in The Second USENIX Workshop on Electronic Commerce Proceedings (Nov 1996) pp 1—11

[BAC90] BAČIĆ E. M.: The Canadian Trusted Computer Product Evaluation Criteria, 6th Annual Computer Security Applications Conference, IEEE 1990, p. 188–196

[BIH96] E Biham, A Shamir, ``Differential Fault Analysis: Identifying the Structure of Unknown Ciphers Sealed in Tamper-Proof Devices", preprint, 10/11/96

[BIE90] Bieber, P.: A Logic of Communication in Hostile Environment, The Computer Security Foundations Workshop III, IEEE 1990, p. 14–22

[BIS88] Bic, L., Shaw, A. C.: The Logical design of Operating Systems, Prentice-Hall, New Jersey 1988

[BLA79] Black Henry C.: Black's Law Dictionary. West Publishing. 1979.

[BLP96A] Bell, D. E., LaPadula, L. J.: Secure Computer System: Mathematical Foundations, Mitre TR 2547 volume I, Mitre 1996

[BLP96B] Bell, D. E., LaPadula, L. J.: Secure Computer System: A Mathematical Model, Mitre TR 2547 volume II, Mitre 1996

[BOY92] Boyd, C.: A Formal Framework for Authentication, Computer Security – ESORICS 92, Springer-Verlag, Berlin 1992, p. 273–292

[BW81] The Spreading Danger of Computer Crime, Business Week, April 20, 1981

[CAL86] Carlson, R. A., Lunt, T. F.: The Trusted Domain Machine: A Secure Communication Device for Security Guard Applications, Security and Privacy Volume 2, Proceedings of the 6th, 7th and 8th Symposia 1985–1987, IEEE 1990, p. 182–186

[CFM95] Castano, S., Fugini, M. G. Martella, G., Samarati, P.: Database Security, Addison-Wesley Publishing Company 1995

[CHA90] Chaum, D. Fiat, A. Naor, M., Untraceable electronic cash. (Springer-Verlag, Berlin, West Germany, p. 319-27, 1990)(Conference: Advances in Cryptology - CRYPTO '88. Proceedings, Santa Barbara, CA, USA, 21-25 Aug. 1988)

[CLW87] Clark, D. C., Wilson, D. R.: A Comparison of Commercial and Military Computer Security Policies, Security and Privacy Volume 2, Proceedings of the 6th, 7th and 8th Symposia 1985–1987, IEEE 1990, p. 184–194

[COL] The Colossus Rebuild Project by Tony Sale, http://www.codesandciphers.org.uk/lorenz/rebuild.htm

[COO90] Cooper, J, A.: Computer and Communications Security, McGraw-Hill Book Company, 1989

[COU77] Courtney, R.: Security risk assessment in electronic data processing, AFIPS Conference Proceedings of the National Computer Conference, AFIPS, Arlington, Va., 97-104

[COW94] Courtney, R. H., Ware, W. H.: What Do We Mean by Integrity?, Computers & Security 13, Elsevier Science Ltd. 1994, p. 206–208

[CRA96] CRAMM Version 3 Description, Insight Consulting, Surrey, 1996

[CUM87] Cummings, P. T.: Compartmented Mode Workstation: Results through Prototyping, Security and Privacy Volume 2, Proceedings of the 6th, 7th and 8th Symposia 1985–1987, IEEE 1990, p. 2–12

[CUR90] Curry D. A.: Improving the Security of your UNIX System, ITSTD-721-FR-90-21, SRI International, April 1990

[CUS93] Custer, H.: Inside Windows NT, Microsoft Press, Washington 1993

[DAL92] D'Ausbourg, B., Llareus, J.: M2S: A Machine for Multilevel Security, Computer Security – ESORICS 92, Springer-Verlag, Berlin 1992, p. 373–391

[DEN86] Denning, D. E.: An Intrusion-Detection Model, Security and Privacy Volume 2, Proceedings of the 6th, 7th and 8th Symposia 1985–1987, IEEE 1990, p. 118–131

[DEN97] Dennison, M. W. L.: A Methodology for Security Policy Modeling, 9th Annual Canadian Information Technology Security Symposium, Ottawa 1997

[DIO81] Dion L. C.: A Complete Protection Model, Security and Privacy Volume 1, Proceedings of the First Five Symposia 1980–1984 , IEEE 1990, p. 49–55

[DOR86] Dobson, J. E., Randell, B.: Building Reliable Secure Computing Systems Out of Unreliable Insecure Components, Security and Privacy Volume 2, Proceedings of the 6th, 7th and 8th Symposia 1985–1987, IEEE 1990, p. 187–193

[ELB93] Eloff, J. H. P. Labuschagne, L., Badenhorst, K. P.: A comparative framework for risk analysis methods, Computers & Security 12, Elsevier Science Ltd. 1993, p. 597–603

[EVE87] Even, S., Secure off-line electronic fund transfer between nontrusting parties. (North-Holland, Amsterdam, Netherlands, p. 57-66, 1989) (Conference: Smart Card 2000: The Future of IC Cards. Proceedings of the IFIP WG 11.6 International Conference, Laxenburg, Austria, 19-20 Oct. 1987)

[FER96] Final Evaluation Report: Windows NT Workstation and Server, Version 3.5 with U.S. Service Pack 3, NCSC–FER–95/003, NCSC 1996

[FOR94] Ford, W.: Computer Communication Security, ISBN 13–799453–2, Prentice Hall 1994

[FOR98] Ford, W., Baum, M. S.: Secure Electronic Commerce, Prentice Hall, 1998

[GAR95] Garfinkel S.: PGP, Pretty Good Privacy, O´ Reilly & Associates, Inc., 1995

[GAS88] Gasser, M.: Building a Secure Computer System, Van Nostrand Reinhold, New York, 1988, ISBN 0-442-23022-2

[GHO98] A. K. Ghosh, E-commerce security, John Wiley, 1998

[GJW91] Gove, R. A., Jaworski, L. M., Willians, J. G.: To Bell and Back: Developing a Formal Security Policy Model for a C2 System, 7th Annual Computer Security Applications Conference, IEEE 1991, p. 143–151

[GRA90] Gray, J. W.: Information Sharing in Secure Systems, The Computer Security Foundations Workshop III, IEEE 1990, p. 128–138

[HAR93] Hardy, G.: Commercial Accreditation of Information Security, Computers & Security 12, Elsevier Science Ltd. 1993, p. 716–729

[HOM96] Honigová, A., Matyáš, V.: Anglicko-česká terminologie bezpečnosti informačních technologií, Computer Press, Praha 1996

[JOH95] Johnson, J. Z.: Risk Management – Theory and Practice, Trident Data Systems, TDS 1995

[LAC84] Landwehr, C. E., Carroll, J. M.: Hardware Requirements for Secure Computer Systems: A Framework, Security and Privacy Volume 1, Proceedings of the First Five Symposia 1980–1984 , IEEE 1990, p. 34–39

[LAC96] G. Lacoste, SEMPER: A Security Framework for the Global Electronic Marketplace, SEMPER document 431LG042, IBM France, August 1996

[LIP82] Lipner, S. B.: Non-Discretionary Controls for Commercial Applications, Security and Privacy Volume 1, Proceedings of the First Five Symposia 1980–1984 , IEEE 1990, p. 2–9

[MDS92] McDermid, J. A., SHI, Q.: Security Composition of Systems, 8th Annual Computer Security Applications Conference, IEEE 1992, p. 112–122

[MHM86] McHugh, J., Moore, A. P.: A Security Policy and Formal Top Level Specification for a Multi-level Secure Local Area Network, Security and Privacy Volume 2, Proceedings of the 6th, 7th and 8th Symposia 1985–1987, IEEE 1990, p. 34–39

[MLE87] McLean, J. D.: Reasoning about Security Models, Security and Privacy Volume 2, Proceedings of the 6th, 7th and 8th Symposia 1985–1987, IEEE 1990, p. 123–130

[MLE90A] McLean, J. D.: Security Models and Information Flow, Proceedings of the 1990 IEEE Symposium on Research in Security and Privacy, IEEE 1990

[MLE90B] McLean, J. D.: The Specification and Modeling of Computer Security, Computer, Vol. 23, No. 1, Jan. 1990, p. 9–16

[MPS93] Muftic, S., Patel, A., Sanders, P., Colon, R., Heijnsdijk, J., Pulkkinen, U.: Security architecture for Open Distributed Systems, John Wiley & Sons 1993

[NOV98] Novák, L.: Příspěvek k teorii bezpečnosti složených systémů důvěryhodných aplikací, disertační práce, VA Brno, 1998

[PAR76] Parker, D.: Crime by Computer, Charles Scribner's Sons, New York, 1976

[PFL91] Pfleeger, C.P.: Security in Computing, Prentice Hall, Englewood Cliffs, NJ (1991)

[ROC90] Roe, M., Casey, T.: Integrating Cryptography in the Trusted Computing Base, 6th Annual Computer Security Applications Conference, IEEE 1990, p. 50–55

[RPJ96] Rábová, Z., Peringer, P., Janoš, J: Simulation Techniques in Information System Design, Workshop'96, Technical University in Prague, Technical University in Brno, 1996

[RUE96] Ru, W.G., Eloff J.H.P.: Risk analysis modelling with the use of fuzzy logic, Computer & Security, Vol. 15, No. 3, pp. 239-248

[SEN96] I. Sendrovic, Security of Electronic Money, Report by the Committe on Payment and Settlement Systems and the Group of Computer Experts of Central Banks of Group of Ten Countries (G-10), Basilej, ISBN 92-9131-119-7, 1996

[SHA49] Shannon, C. E.: Communication Theory of Secrecy System, Bell System Techn. J., 28, No 4 (1949), p. 656–715, ruský překlad

[SHG91] Shieh, S. W., Gligor, V. D.: A Pattern-Oriented Intrusion-Detection Model and Its Applications, 1991 IEEE Computer Society Symposium on Research in Security and Privacy, IEEE 1991, p. 327–342

[SCH94] Schneier, B.: Applied Cryptography: Protocols, Algorithms and Source Code, ISBN 0–471–59756–2, John Wiley & Sons 1994

[SPI88] Spivey J. M.: The Z notation: A Reference Manual, Prentice Hall International, 1988.

[TUN87] Tunstall, J.S., Electronic currency. (North-Holland, Amsterdam, Netherlands, p. 47-8, 1989) (Conference: Smart Card 2000: The Future of IC Cards. Proceedings of the IFIP WG 11.6 International Conference, Laxenburg, Austria, 19-20 Oct. 1987)

[ZAM97] Zámečník M., Kosiner I., Papp R., Seiner M.: Problematika ochrany zdravotnických dat, klasifikace citlivosti zdravotnických dat a doporučené

bezpečnostní funkce pro jejich přenos, Verze 1.0, Ministerstvo zdravotnictví ČR, 1997

7.2 Seznam použitých norem a standardů

[BSI] Code of Practice for Information Security Management, BS 7799, BSI 1995

[BS7799] ČSN ISO/IEC 17799, Informační technologie - Soubor postupů pro řízení informační bezpečnosti, ČSNI Praha

[CC94] Common Criteria for Information Technology Security Evaluation (version 0.9): Preliminary DRAFT, ISO 1994

[CC96] Common Criteria for Information Technology Security Evaluation (version 1.0), ISO 1996

[CC98] Common Criteria for Information Technology Security Evaluation (version 2.0), ISO 1998

[CC] ISO/IEC 15408, Information technology – Security techniques – Evaluatution criteria for IT security, v české verzi ČSN ISO/IEC 15408

[CTCPEC] The Canadian Trusted Computer Product Evaluation Criteria (version 3.0e), CSE, Ottawa 1993

[DTR] Derived Test Requirements (DTR) for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology

[FC] Federal Criteria for Information Technology Security, Volume I and II, US National Institute of Standards and Technology & National Security Agency, December 1992

[FIPS1401] Security Requirements for Cryptographic Modules, FIPS PUB 140-1, Federal Information Processing Standards Publication, National Institute of Standards and Technology, U.S. Department of Commerce, January 11, 1994

[FIPS140] Security Requirements for Cryptographic Modules, FIPS PUB 140-2, Federal Information Processing Standards Publication, National Institute of Standards and Technology, U.S. Department of Commerce, May 25, 2001

[ISO7498] ISO 7498-2 Information Processing Systems, Open Systems Interconnection, 2: Security Architecture, 1988

[ITSEC] Information Technology Security Evaluation Criteria (ITSEC), Office for Official Publications of the European Communities, Luxembourg 1991, ISBN 92-826-3004-8

[ITSECcz] Kritéria hodnocení bezpečnosti informačních systémů (ITSEC): Prozatímní harmonizovaná kritéria, European Communities, překlad MH ČR, Praha 1993

[ITSEM] Information Technology Security Evaluation Manual (ITSEM), Office for Official Publications of the European Communities, Luxembourg 1994, ISBN 92-826-7087-2

[ITSEMcz] Návod pro hodnocení bezpečnosti v informačních technologiích (ITSEM): Prozatímní harmonizovaná metodologie, European Communities, překlad MH ČR, Praha 1994

[ITSICH] IT-Sicherheitskriterien: Kriterien für die Bewertung der Sicherheit von Systemen der Informationstechnik (IT), Zentralstelle für Sicherheit in der Informationstechnik, Bonn, ISBN 3-88784-192-1

[MSFR] Minimum Security Functionality Requirements for Multi-User Operating Systems, Computer Security Division, Computer Systems Laboratory, US National Institute of Standards and Technology, Issue 1, January 28, 1992

[NCS88] National Computer Security Center: Glossary of Computer Security Terms-NCSC-TG-004. Government Printing Office. 1988

[NCS92] A Guide to Understanding Security Modeling in Trusted Systems, NCSC-TG-010, National Computer Security Center, 1992.

[NIST800] Security Issues in the Database Language SQL, NIST PUB 800-8, Nationa Institute of Standards and Technology, 1993

[PP9806] PP/9806 - Smartcard Integrated Circuit Protection Profile v2.0

[PP9809] PPnc/9809 - Smartcard Integrated Circuit with Embedded Software

[PP9810] PP/9810 - Smartcard Embedded Software v1.2

[PP9911] PP9911 - Smartcard Integrated Circuit with Embedded Software v2.0

[PPCIMC] Certificate Issuing and Management Components Protection Profile, NIST PKI Project Team, January 26, 2001

[RFC1825] Atkinson, R.: Security Architecture for the Internet Protocol, RFC 1825

[RFC1826] Atkinson, R.: IP Authetication Header, RFC 1826

[RFC1827] Atkinson, R.: IP Encapsulating Security Payload, RFC 1827

[RFC 2510] Certificate Management Protocols, RFC 2510

[RFC 2511] Internet X.509 Certificate Request Message Format, RFC 2511

[RFC 2459] Certificate and CRL Profile, RFC 2459

[RFC 2527] Certificate Policy and Certification Practices Framework, RFC 2527

[RFC 2528] Representation of Key Exchange Algorithm (KEA) Keys in Internet X.509 Public Key Infrastructure Certificates, RFC 2528

[RFC 2559] Operational Protocols - LDAPv2, RFC 2559

[RFC 2560] Online Certificate Status Protocol - OCSP, RFC 2560

[RFC 2585] Operational Protocols: FTP and HTTP, RFC 2585

[RFC 2587] LDAPv2 Schema, RFC 2587

[RFC 2797] Certificate Management Messages over CMS, RFC 2797

[RFC 2802] Digital Signatures for the v1.0 Internet Open Trading Protocol (IOTP), RFC 2802

[RFC 2807] XML Signature Requirements, RFC 2807

[RFC 3039] Qualified Certificate Profile, RFC 3039

[RFC 3161] Time-Stamp Protocol (TSP), RFC 3161

[RFC 3279] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, RFC 3279

[RFC 3280] Certificate and Certificate Revocation List (CRL) Profile, RFC 3280

[RFC 3281] An Internet Attribute Certificate Profile for Authorization, RFC 3281

[SCPP] Smart Card Security User Group - Smart Card Protection Profile, Version 3.0, BSI-PP-0003-2001 (10.10.2001)

[SMIME] S/MIME Implementation Guide Interoperability Profiles, Version 2, S/MIME Editor, Draft, Revised October 8, August 28, 1996

[STE96] Secure Electronic Transaction Technical Specification, VISA, MasterCard, 1996

[TCSEC] Trusted Computer Systems Evaluation Criteria, DOD 5200.28-STD, Department of Defense, United States of America, December 1985.

[TCSEScz] Kritéria hodnocení zabezpečených počítačových systémů, CSC–STD–001–83, český překlad, BEN, Praha 1994

[TG0188] A Guide to Understanding Audit in Trusted Systems, NCSC–TG–001, June 1988

[TG0387] A Guide to Understanding Discretionary Access Control in Trusted Systems, NCSC–TG–003, September 1987

[TG0488] Glossary of Computer Security Terms, NCSC–TG–004, October 1988

[TG08] Trusted Distribution Manual, NCSC-TG-008, Library No. S-228.592

[TG1092] A Guide to Understanding Security Modeling in Trusted Systems, NCSC–TG–010, October 1992.

[TG2191] Trusted Database Management System Interpretation of the Trusted Computer System Evaluation Criteria, NCSC–TG–021, April 1991

[TR13335] ISO/IEC JTC1/SC27 TR 13335: Guidelines for the Management of IT Security

[TR15446] ISO/IEC PDTR 15446: Information technology – Security techniques – Guide for the production of protection profiles and security targets

[VME95] Integrated Circuit Card Specifications for Payment Systems, VISA, MasterCard, Europay, 1995

[ZOEP] Zákon č. 227/2000 Sb., o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění zákona č . 226/2002 Sb.

[ZOEPV] Vyhláška č. 366/2001 Sb., o upřesnění podmínek stanovených v § 6 a 17 zákona o elektronickém podpisu a o upřesnění požadavků na nástroje elektronického podpisu.

7.3 Seznam vlastních publikací autora se vztahem k tématu práce

Původní článek v mezinárodním vědeckém časopise

[HAN98a] Hanáček, P.: Security of Electronic Money, In: Lecture Notes in Computer Science, č. 1521, Springer-Verlag, 1998, s.107-121, ISSN 0302-9743 (impact factor 0.415)

Původní příspěvek ve sborníku mezinárodní vědecké konference

[HRA97a] Hanáček P., Rábová Z.: Risk Analysis Model of Information System, Proceedings of Conference MOSIS'97, April 1997, Hradec nad Moravicí, Czech Republic, pp 169-174 (50%)

[HRA97b] Hanáček P., Rábová Z.: Processing of Input Data for Risk Analysis, Proceedings of Conference ASIS'97, September 1997, Krnov, Czech Republic, pp 91-96, (50%)

[HRA98a] Hanáček, P., Rábová, Z.: Knowledge-Based Simulation in Risk Analysis, In: Proceedings of ASIS 1998, MARQ, Krnov, 1998, s.79-84, ISBN 80-85988-26-7 50%

[HAN98b] Hanáček, P.: Security of Smartcard Based Payment Protocol, In: Proceedings of International Conference MOSIS'98, MARQ, Bystrice pod Hostynem, 1998, s.123-129, ISBN 80-85988-24-0

[HAN99a] Hanáček Petr: Security Verification of Smartcard Scripts, In: ISM'99, Roznov pod Radhostem, MARQ, 1999, p. 11-18, ISBN 80-85988-31-3

[HAN99a] Hanáček Petr: Implementing Secure Payment Systems to Avoid Potential Problems, In: Banking Technology in Central europe, Praha, 1999, p. 6

[HRA99a] Hanáček Petr, Rábová Zdeňka: Interactive Tools for Creation of Assets Model, In: ASIS 1999, Krnov, MARQ, 1999, p. 213-219, ISBN -80-85988-41-0 50 %

[HAN00a] Hanáček Petr: Problems of Tamper Resistant Software, In: ISM 2000, Roznov pod Radhostem, MARQ, 2000, p. 117-122

[HPR00] Hanáček Petr, Peringer Petr, Rábová Zdeňka: Knowledge-Based Approach to Risk Analysis Modelling, In: Proceedings of JCKBSE 2000, Brno, 2000, p. 25-30, ISBN 1-58603-060-4 33 %

Původní příspěvek ve sborníku národní vědecké konference

- Hanáček P., Staudek J.: Informační systémy a jejich bezpečnost, Programování '92, 26.5.-28.5.1992 Ostrava, sborník str. 114-130, pořadatel - Dům techniky ČSVTS Ostrava, 50%
- Hanáček P.: Hodnocení a klasifikace bezpečnosti informačních systémů, seminář Programování '93, 8.6.-10.6. 1993 Ostrava, sborník strana 168-176, pořadatel - Dům techniky ČSVTS Ostrava
- Hanáček P.: Modely bezpečnosti informačních systémů, XVI. moravskoslezské mezimárodní kolokvium Vybrané problémy simulačních modelů, Kat. inf. FEI VŠB, CSS, SCS, EUROSIM, Brno 6.-8.9. 1994, str. 35-39
- Hanáček P.: Bezpečnost informačních systémů, Seminář INFORMATIKA 94, Tábor 4.-5. května 1994, sborník str. 13-18
- Hanáček, P.: Kritéria hodnocení bezpečnosti ITSEC a cesta k nim, seminář "HODNOCENÍ INFORMAČNÍ BEZPEČNOSTI", Praha 1995, str. IV-1 až IV-7
- Hanáček, P.: Hodnocení bezpečnosti kryptografických modulů, seminář "HODNOCENÍ INFORMAČNÍ BEZPEČNOSTI", Praha 1995, str. XI-1 až XI-4
- Hanáček, P.: Bezpečnost v informačních systémech, konference DATASEM'95, sborník strana 29-38, CS-Compex Brno, 1995
- Hanáček, P.: Problémy bezpečnosti při tvorbě informačních systémů, seminář "Některé nové přístupy při tvorbě informačních systémů", Brno 10.-14. října 1995
- Hanáček, P.: Zdravotnická dokumentace a ochrana dat, Kongres MEFA'96, 6.-9. 11. 1996, Česká lékařská společnost J.E. Purkyně, Brno
- Hanáček, P.: Ochrana dat a bezpečnost informačních systémů, Konference MEDSOFT'96, Praha 1996, str. 11-20
- Hanáček, P.: Problémy bezpečnosti při implementaci informačních systémů, Letní škola "Informační systémy a jejich aplikace", Studnice 3.-6. září 1996, str. 26-32
- Hanáček, P.: Bezpečnost a ochrana informací při elektronickém platebním styku, Seminář "Ochrana a bezpečnost informací v informačních systémech", Brno 1.-4.4. 1996, str. 68-77
- Hanáček, P.: Rizika surfování po vlnách Internetu, Seminář Virus'96, 14.-15. 5. 1996, Praha, 11 stran
- Hanáček, P.: Informační bezpečnost a Internet, Seminář AFOI'96, 20. 2. 1996, Praha, 11 stran

- Hanáček, P.: Problémy bezpečnosti při implementaci informačních systémů, Konference RADAR'96, Brno, 17.9. 96, 7 stran
- Hanáček, P.: Elektronický podpis a jeho využití v informačních systémech, Konference Bezpečnost a ochrana informací v informačních a komunikačních systémech, Brno, 5.-7.5. 1997, pp. 93-99
- Hanáček, P., Staudek, J.: Bezpečnostní politika IS v prostředí Internet, 17. ročník databázové konference DATASEM'97, Brno, 12.-14. říjen 1997, ISBN 80-238-1176-2, pp. 1-26 (50%)
- Hanáček, P.: Přenos medicínských dat po veřejných sítích, Seminář MEDSOFT'97, Jihlava 1997, pp. 19-21
- Hanáček, P.: Bezpečnost komunikace v síti Internet, Seminář COMPEX'97, květen 1997, Ostrava, 9 stran
- Hanáček, P.: Internet a bezpečné protokoly, 5. seminář AFOI Internet a informační bezpečnost, únor 1997, Praha, pp. 33-40
- Hanáček, P., Staudek, J.: Bezpečnost distribuovaných systémů, In: Sborník konference DATASEM'98, CS COMPEX, Brno, 1998, s.1-20 50%
- Hanáček, P., Staudek, J.: Zabezpečení přenosu zdravotnických informací, In: Sborník konference MEDSOFT'98, TECH-MARKET, Vlašim, 1998, s.9-15, ISBN 80-86114-17-1 50%
- Hanáček, P.: Metodika vytváření bezpečnostní politiky připojení k síti Internet, In: Sborník semináře AFOI 1998, Agentura ACTION-M, Praha, 1998, s.7
- Hanáček, P.: Platby v elektronickém obchodu, In: Sborník konference VIRUS'98, AEC Brno, Praha, 1998, s.65-79
- Hanáček, P., Rábová, Z., Kotyza, B.: Znalostní model analýzy rizik, In: Sborník letní školy Informační systémy a jejich aplikace 1998, Ústav automatizace inženýrských úloh a informatiky FAST VUT Brno, Ruprechtov, 1998, s.213-219, ISBN 80-214-1205-4 30%
- Hanáček, P.: Bezpečnost čipových karet..., In: Sborník letní školy Informační systémy a jejich aplikace 1998, Ústav automatizace inženýrských úloh a informatiky FAST VUT Brno, Ruprechtov, 1998, s.49-61, ISBN 80-214-1205-4
- Hanáček Petr: Proč potřebujeme zákon o digitálním podpisu, In: Seminář AFOI, Praha, 1999, p. 67-70
- Hanáček Petr, Staudek Jan: Bezpečnost elektronického obchodu, In: Systems Integration '99, Praha, 1999, p. 55-74, ISBN 80-7079-059-8 50 %
- Hanáček Petr: Bezpečnost systémů informační společnosti, In: Sborník konference RUFIS'99, Brno, VUT v Brně, 1999, p. 23-28, ISBN 80-214-1379-4

- Hanáček Petr, Hanzal Martin, Rábová Zdeňka: Interaktivní budování modelu aktiv, In: Sborník LŠ Informační systémy a jejich aplikace, Ruprechtov, 1999, p. 60-69, ISBN 80-214-1379-2 33 %
- Hanáček Petr: Bezpečnost informačních systémů, In: ASIS 1999, Krnov, MARQ, 1999, p. 11-19, ISBN 80-85988-41-0
- Hanáček Petr: Digitálni podpis elektronické dokumentace, In: Brno, 1999
- Hanáček Petr: Výuka bezpečnosti informačních systémů, In: Studnice, 1999, p. 23-27, ISBN 80-85615-79-1
- Hanáček Petr, Staudek Jan: Bezpečnost informačních systémů, Praha, 2000, p. 127, ISBN 80-238-5400-3 50 %
- Hanáček Petr: Digitální podpis zdravotnické dokumentace, Lékař a technika, Praha, 2000, p. 130-132
- Hanáček Petr: Certifikace veřejných klíčů a certifikační autority, In: Sborník konference Security'2000, Praha, 2000, p. 86-88
- Hanáček Petr: Elektronický podpis jako nástroj bezpečného obchodování, In: Sborník konference Internet jako nástroj obchodního úspěchu, Brno, 2000, p. 10
- Hanáček Petr: Certifikace veřejných klíčů a podpora legislativy, In: Sborník semináře elektronický podpis, Praha, 2000, p. 43-47
- Hanáček Petr: Hodnocení bezpečnosti podle normy ISO/IEC 15408, In: Sborník konference AFOI 2000, Praha, 2000, p. 10
- Češka Milan, Hanáček Petr, Hruška Tomáš, Rábová Zdeňka, Zbořil František: Návrh bakalářského programu Informační technologie na VUT v Brně, In: Proceedings of workshop CSEW 2000, Liblice, 2000, p. 42-48, ISBN 80-01-02264-1 20 %
- Hanáček Petr: Bezpečnost elektronického obchodování - rizika, In: Praha, 2000, p. 12
- Hanáček Petr: Technicko-právní aspekty a ochrana elektronických dokladů, In: Institut of International Research, Praha, 2001, p. 10
- Hanáček Petr, Staudek Jan: Infrastruktura certifikace veřejných klíčů, In: Security and Protection of Information 2001, Brno, 2001, p. 79-86 50 %
- Hanáček Petr: Rizika elektronického obchodu, In: SECURITY 2001, Brno, 2001, p. 48-54
- Hanáček Petr: Bezpečnost transakcí na internetu, In: Moderní databáze, Praha, KOMIX, 2001, p. 76-83, ISBN 80-238-7046-7
- Hanáček Petr, Staudek Jan: Certifikační infrastruktury veřejných klíčů, In: Proceedings of DATAKON 2001, Brno, FEI STUBA, 2001, p. 1-44, ISBN 80-227-1597-2 50 %

- Hanáček Petr: Bezpečnost mobilních zařízení ve světle nových aplikací, In: Sborník konference Security 2002, Praha, 2002, p. 39-46
- Hanáček Petr: Bezpečnost čipových karet proti útokům, In: Sborník konference SmartWorld 2002, Zlín, 2002, p. 20
- Hanáček Petr: Hodnocení bezpečnosti IT podle normy ISO/IEC 15408, In: Sborník konference Informační bezpečnost - teorie a praxe, Brno, 2002, p. 10
- Hanáček Petr: Zabezpečení elektronických transakcí v prostředí internetu, In: Sborník konference Trendy IT Security, Praha, 2002, p. 20
- Rábová Z., Hanáček P.: Model analýzy rizik informačního systému, letní škola Informační systémy a jejich aplikace, FAST VUT Brno, Ruprechtov, 16-19. září 1997, s. 30-34 (50%)
- Hanáček Petr: Bezpečnost elektronických transakcí, In: Proceedings of Conference e-Finance, Praha, 2001, p. 10
- Hanáček Petr, Zbořil František ml.: Řízení rizik v procesu Analýzy rizik, In: Proceedings of the 35th Spring International Conference MOSIS'01, Ostrava, MARQ, 2001, p. 351-356, ISBN 80-85988-57-7 50 %
- Hanáček Petr, Rábová Zdeňka: Využití modelování v analýze rizik, In: Proceedings of the 23rd International Autumn Colloquium ASIS 2001, Ostrava, MARQ, 2001, p. 9-16, ISBN 80-85988-61-5 50 %
- Hanáček Petr, Rábová Zdeňka: Využití modelů při analýze rizik, In: Proceedings of ASIS 2002, Ostrava, MARQ, 2002, p. 9-16, ISBN 80-85988-77-1 50 %
- Hanáček Petr: Elektronický podpis a PKI v platebních systémech, In: Sborník konference Bezpečnosť informácií vo finančnom sektore, Žilina, NMC, 2002, p. 21-26, ISBN 80-85655-20-9

Článek v odborném časopise

- Hanáček P., Staudek J.: Viry - hrozby pro počítače, díl 1, Computer Echo 6/93, 10 stran, 50%
- Hanáček P., Staudek J.: Viry - hrozby pro počítače, díl 2, Computer Echo 1/94, 6 stran, 50%
- Hanáček P., Staudek J.: Viry - hrozby pro počítače, díl 3, Computer Echo 2/94, 5 stran, 50%
- Hanáček P., Staudek J.: Antivirové programy, Computer Echo 4/94, 8 stran, 50%
- Hanáček P.: Bezpečnost v systému Windows NT, PC MAGAZINE, červenec 1994, str. 124-131
- Hanáček P.: Hodnocení bezpečnosti informačních systémů podle kritérií ITSEC, Magazín ČSN č. 7-8/1994

- Hanáček P.: Alternativa ke smartkartě - SMARTDISK, Bulletin AFOI, č. 1/1994, str. 6
- Hanáček P.: Bezpečnost informačních systémů - hodnocení bezpečnosti a certifikace podle kritérií ITSEC, Bulletin AFOI, č. 2/1994, str. 11-12
- Hanáček, P.:"Clipper - konec práva občanů na soukromí", Bulletin AFOI, číslo 2/95, str. 8
- Hanáček, P.:"Průmyslové aplikace elektronického podpisu", Bulletin AFOI, číslo 2/95, str. 16-17
- Hanáček, P.:"Certifikace Windows NT pro třídu C2", Bulletin AFOI, číslo 2/95, str. 16-17
- Hanáček, P.: Hodnocení bezpečnosti kryptografických modulů, ComputerWorld č. 29/1995, str. 29-30
- Hanáček, P.: Kritéria hodnocení bezpečnosti ITSEC a cesta k nim, ComputerWorld č. 30/1995, str. 29-30
- Hanáček, P.: Standardy bezpečnosti IT, ComputerWorld 34/97, strana 14, ISSN 1210-9924
- Hanáček, P.: Šifrovací algoritmus DES, ComputerWorld 36/97, strana 14, ISSN 1210-9924
- Hanáček, P.: Zdravotnická dokumentace a ochrana dat, Lékař a technika č. 5/1997, pp. 111-113, ISSN 0301-5491, INDEXED IN EMBASE

Standardy

- Hanáček, P., Staudek, J.: Vytvoření standardu Ministerstva zdravotnictví ČR "Bezpečnostní funkce pro zabezpečení přenosu zdravotnických informací", Ministerstvo zdravotnictví ČR, listopad 1996, 75 stran, podíl 50%

Knihy

[HS94a] Staudek J., Hanáček P.: Bezpečnost informačních systémů - příručka pro projektanty a správce informačních systémů ve státní správě ČR, zakázka ministerstva hospodářství ČR, 1994, 150 stran, 50%

[Kol96a] Kolektiv autorů: Jak publikovat na počítači, Nakladatelství Science, Veletiny 1996, ISBN 80-901475-77, podíl 14 %

[BMH97] Berka, M., Macur, J., Hanáček, P.: WWW informační servery, UNIS Edition Brno 1997, 158 stran, (25%)

[HS00a] Hanáček, P., Staudek, J.: Bezpečnost informačních systémů, ÚSIS, Praha, 2000, s. 127, ISBN 80-238-5400-3, 50%

Překlady odborných knih

- Hanáček P., Staudek J.: Harmonizovaná kritéria pro hodnocení bezpečnosti informačních technologií, příručka pro správce informačních systémů, Ministerstvo průmyslu, srpen 1993 č. 011-032/3, 163 stran, 50%

- Hanáček P., Staudek J.: Překlad publikace Návod pro hodnocení bezpečnosti v informačních technologiích (ITSEM), Ministerstvo hospodářství ČR, 50%

Oponované výzkumné zprávy

- Hanáček, P.: Metodologie bezpečnosti informačních systémů, oponovaná výzkumná zpráva GAČR 102/94/1097, 1997, 29 stran

8. Přílohy

8.1 Příloha A - Příklad osnovy CP a CPS

Obsah dokumentů CP a CPS by měl odpovídat zvyklostem a standardům pro vypracovávání těchto dokumentů, běžným ve světě. Základní osnova je stejná pro oba dokumenty (CP i CPS) a měla by zahrnovat následující kapitoly:

1. Úvod

Tato kapitola definuje, kdo provozuje a spravuje CA, kterým uživatelům CA slouží jak ji lze kontaktovat.

2. Obecné požadavky na zúčastněné strany

Tato kapitola definuje práva, povinnosti, zodpovědnosti, vztah ke státní správě a zákonům a podobné požadavky. Může se skládat například z těchto podkapitol:

- Povinnosti jednotlivých stran
- Prosazení CP a řešení problémů
- Zveřejnění certifikátů a repositář
- Audit dodržování CP a CPS
- Důvěrnost informací

3. Identifikace a autentizace žadatelů

Tato kapitola se zabývá tím, jak jsou uživatelům přiřazována jména (identifikátory) a jak je ověřována jejich identita. Může se skládat například z těchto podkapitol:

- Počáteční registrace žadatele o certifikát
- Opětovné vydání certifikátu
- Požadavek na zrušení certifikátu

4. Provozní požadavky

Popisuje proces vydávání a rušení certifikátů, záznamy, které je třeba vést, prováděný audit a postupy zotavení po bezpečnostním incidentu. Může se skládat například z těchto podkapitol:

- Žádost o certifikát
- Vydání certifikátu
- Pozastavení a zrušení certifikátu
- Procedury bezpečnostního auditu

- Archivace záznamů
- Změna klíčů CA
- Zotavení po bezpečnostním incidentu
- Ukončení činnosti CA

5. Fyzické, procedurální a personální opatření

Popisuje bezpečnostní opatření, implementovaná v CA. Zahrnuje tyto podkapitoly:

- Fyzická bezpečnost
- Procedurální bezpečnost
- Personální bezpečnost

6. Technická bezpečnostní opatření

Tato kapitola pokrývá kryptografické mechanismy, generování klíčů, použité algoritmy, ochranu kryptografických klíčů a technické bezpečnostní požadavky na CA a uživatele certifikátů. Může se skládat například z těchto podkapitol:

- Generování klíčů
- Ochrana soukromých klíčů
- Správa klíčů
- Bezpečnost počítačového vybavení
- Bezpečnost životního cyklu vybavení
- Síťová bezpečnost
- Bezpečnost kryptografických modulů

7. Profily certifikátů a CRL

Tato kapitola definuje použité položky certifikátů a CRL, použitá rozšíření, jejich význam a způsob jejich využívání. Obsahuje dvě podkapitoly:

- Profil certifikátu
- Profil CRL

8. Správa certifikační politiky / Správa CPS

Tato kapitola popisuje způsob administrace a udržování CP a CPS.

8.2 Příloha B – Příklad struktury SBP

Systémová bezpečnostní politika specifikuje množinu zákonů, pravidel a praktik, které určují, jakým způsobem jsou organizovány, chráněny a distribuovány uvnitř daného systému citlivé informace a jiné zdroje. Musí určovat bezpečnostní cíle systému a možné hrozby. Bezpečnostní cíle musí být plněny konkrétními bezpečnostními funkcemi a pomocí fyzických, personálních nebo procedurálních postupů, které se vztahují k systému. Systémová bezpečnostní politika musí pokrýt všechny aspekty bezpečnosti hodnoceného systému, včetně souvisejících fyzických, personálních a procedurálních bezpečnostních opatření.

Systémová bezpečnostní politika může mít například následující strukturu:

1. Úvod
2. Všeobecné informace
   - 2.1 Účel dokumentu
   - 2.2 Rozsah a platnost dokumentu
   - 2.3 Požadavky bezpečnosti dané legislativou
3. Popis systému
   - 3.1 Určení systému
   - 3.2 Softwarové komponenty systému
   - 3.3 Datové komponenty systému
   - 3.4 Hardwarové komponenty systému
   - 3.5 Provozní prostředí systému
     - 3.5.1 Fyzické umístění systému
     - 3.5.2 Režim provozu systému
     - 3.5.3 Rizika provozního prostředí
   - 3.6 Typy dat v systému
     - 3.6.1 Charakter dat
     - 3.6.2 Klasifikace dat
   - 3.7 Uživatelé systému
     - 3.7.1 Správa uživatelů
     - 3.7.2 Definice kategorií uživatelů
4. Definice hrozeb
   - 4.1 Kategorizace možných útočníků
   - 4.2 Skupina hrozeb 1
   - 4.3 Skupina hrozeb 2
   - 4.4 ...
5. Bezpečnostní funkce
   - 5.1 Fyzické zabezpečení
   - 5.2 Administrativní bezpečnostní funkce
   - 5.3 Technická bezpečnostní opatření
     - 5.3.1 Identifikace a autentizace

8.3 Příloha C – Příklad struktury PKSPO

Dokument „Plán pro zvládání krizových situací a plán obnovy“ (PKSPO) popisuje postupy a činnosti, které je třeba vykonat při vzniku mimořádné události k tomu aby byla událost a její dopady eliminovány a provoz poskytovatele certifikačních služeb obnoven. V plánu je zpracován seznam činností, které se považují za zásadní s uvedeným stupněm priority a časového limitu vykonání.

PKSPO může mít například následující strukturu:

1. ÚVOD
2. ZÁKLADNÍ FUNKCE SYSTÉMU
   - 2.1 Kritické komponenty systému
   - 2.2 Potenciální stavy systému
   - 2.3 Mimořádné události
   - 2.4 Krizový tým
   - 2.5 Servisní společnosti a dodavatelé
3. DETEKCE MIMOŘÁDNÝCH UDÁLOSTÍ
4. PLÁNY ŘEŠENÍ PŘEDPOKLÁDANÝCH MIMOŘÁDNÝCH UDÁLOSTÍ
   - 4.1 Scénář 1
     - Popis situace: xxx
     - Detekce situace: xxx
     - Ovlivněné části systému: xxx
     - Ovlivněné funkce systému: xxx
     - Postup řešení: xxx
     - Čas obnovy: xxx
   - 4.2 Scénář 2
     - Popis situace: xxx
     - Detekce situace: xxx
     - Ovlivněné části systému: xxx
     - Ovlivněné funkce systému: xxx
     - Postup řešení: xxx
     - Čas obnovy: xxx
   - 4.3 ...
5. ÚDRŽBA A REVIZE HAVARIJNÍHO PLÁNU
6. SLOŽENÍ KRIZOVÉHO TÝMU

8.4 Příloha D – Realizace specifikací

Požadované specifikace je třeba na různých úrovních zaručitelnosti realizovat různým způsobem. Jsou definovány tři způsoby vyjádření těchto specifikací: neformální, poloformální a formální. Tyto tři způsoby jsou poměrně precizně definovány, jak si ukážeme v následujících podkapitolách.

Neformální specifikace

Neformální specifikace je zapsána v přirozeném jazyce a ne v notaci, která vyžaduje nějaké speciální omezení nebo dodržování pravidel. Přirozený jazyk je chápán jako pojem pro komunikaci v běžném hovorovém jazyce. Specifikace zapsaná v přirozeném jazyce nepodléhá žádným speciálním omezením, přitom ale musí splňovat obecná pravidla platná pro daný jazyk (například gramatiku a syntaxi).

Specifikace v přirozeném jazyce musí být vyjádřena tak, aby minimalizovala nejednoznačnosti s tím, že (přinejmenším) všechny pojmy jsou užívány konzistentně a každý pojem se speciálním významem (který není uveden v běžně užívaném slovníku) je definován ve výkladovém slovníku. Je pravděpodobné, že nejednoznačnosti nebudou zcela vyloučeny.

Poloformální specifikace

Poloformální způsob specifikace vyžaduje užití některé omezující notace (nebo notací) spolu s množinou konvencí, která je součástí specifikace nebo na ni existuje odkaz. Tyto konvence jsou specifikovány neformálně. Užitá notace musí umožňovat specifikaci jak funkčních efektů, tak všech mimořádných nebo chybových situací náležejících k dané funkci.

Poloformální způsob specifikace může mít buď grafickou podobu, nebo může být založen na omezeném užití přirozeného jazyka (například struktury omezených vět a klíčových slov se speciálním významem). Jako příklady poloformální specifikace mohou sloužit grafy toku dat, diagramy vzájemných vztahů mezi entitami a relacemi, grafy datových struktur, grafy struktury procesu nebo programu, notace SDL doporučená CCITT.

Metody strukturovaného návrhu a vývoje obvykle obsahují alespoň jednu takovou poloformální notaci pro popis požadavků spolu s návodem, jak notaci využívat. Příklady metod strukturovaného návrhu, které obsahují takové notace, jsou: *Yourdon Structured Method, Structured Analysis and Design Technique, Structured Systems Analysis and Design Method, Jackson Structured Design* a *Jackson Structured Programming*.

Zvláštní příklad poloformální notace, který je úspěšně využíván při definování specifikace bezpečnosti, je požadavkový jazyk (Claims Language - CL). Požadavkový jazyk je podmnožina přirozeného jazyka (angličtiny), ve které jsou předepsány slovní a syntaktické formy požadavkových vět. Byl určen, jak naznačuje jeho název, pro vyjádření požadavků na bezpečnostní charakteristiky produktů IT. Požadavkový jazyk přispívá k využívání přirozeného jazyka pro vyjádření požadavků na bezpečnost prosazující funkce.

Formální specifikace

Formální specifikace je zapsána ve formální notaci, která využívá dobře definovaných matematických pojmů. Pomocí těchto pojmů se definuje syntaxe a sémantika použité notace a také dokazovací pravidla sloužící pro logické dokazování. Formální specifikace musí být odvoditelná z množiny axiomů a musí splňovat některé klíčové vlastnosti, jako je existence výsledků výstupů pro všechny možné vstupní podmínky. Pokud je specifikace hierarchická, musí existovat důkaz, že každá následující úroveň zachovává vlastnosti definované v úrovni předcházející.

Syntaktická a sémantická pravidla formální notace, využívaná ve specifikaci bezpečnosti, musí definovat způsob jednoznačného pochopení užitých konstrukcí a k zjištění jejich významu. Je-li pro logické odvození užito pravidel, musí existovat důkaz, že není možno odvodit opak. Všechna pravidla notace musí být definována nebo na jejich definice musí existovat odkaz. Všechny konstrukce užité ve formální specifikaci jsou beze zbytku popsány příslušnými pravidly. Formální notace musí umožnit specifikaci jak funkčních efektů, tak všech mimořádných nebo chybových situací spojovaných s jednotlivými funkcemi.

Příklady formálních notací jsou: metoda *VDM*, *Z notace*, *RAISE Specification Language*, *Gypsy Specification Language*, *ISO Protocol Specification Language*. Použití konstrukcí z predikátové nebo jiné logiky a teorie množin pro formální notaci je možné za předpokladu, že příslušná pravidla jsou dokumentována nebo odkazována.