BIS02 - MNG

Model 2019

Bezpečnost informačních systémů

Část 2

Kritéria hodnocení bezpečnosti IS

Post 18/19

Souhrnné materiály

Ver 0.1

Bezpečnost informačních systémů

Metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií

Petr Hanáček,
Jan Staudek

Úřad pro státní informační systém
2000

2. Bezpečnostní funkce

2.1 Bezpečnostní funkce podle kritérií ITSEC

Kritéria pro hodnocení bezpečnosti IT ITSEC (Information Technology Security Evaluation Criteria) byla vytvořena v roce 1990 a vydána Úřadem pro oficiální publikace Evropského společenství a schválena jako doporučení v dubnu 1995. Jejich rysy a vlastnosti jsou popsány v poslední kapitole příručky.

2.1.1 Třídy funkčnosti ITSEC

Kritéria ITSEC, viz [ITSEC], specifikují sedm *tříd míry zaručitelnosti bezpečnosti IT* označovaných E0 až E6 reprezentujících vzrůstající úrovně důvěry a v příloze definují dalších deset *tříd bezpečnostní funkčnosti* F-xx. Třídy míry zaručitelnosti kladou požadavky na:

- proces vývoje IS
- prostředí vývoje IS
- provozní dokumentace IS
- provozní prostředí IS.

Pět tříd bezpečnostní funkčnosti F-C1, F-C2, F-B1, F-B2 a F-B3 odpovídá stejnojmenným třídám kritérií TCSEC, viz [TCSEC]. Zbylých pět tříd bezpečnostní funkčnosti je orientováno aplikačně. Na rozdíl od TCSEC, která vznikala pro vojenské prostředí a orientovala se zejména na ochranu důvěrnosti informace, jsou ITSEC koncipována mnohem obecněji a pokrývají částečně i požadavky na integritu a na dostupnost informace. Oproti TCSEC definují ITSEC navíc i způsob vedení dokumentace hodnoceného předmětu, způsob definování bezpečnostního cíle a způsob provádění hodnocení.

Zatímco pro požadavky na míru zaručitelnosti bezpečnosti je v kritériích ITSEC definováno sedm tříd míry zaručitelnosti bezpečnosti E0 až E6 a nepředpokládá se, že by uživatelé kritérií definice těchto tříd měnili nebo si definovali své vlastní třídy, u požadavků na bezpečnostní funkčnost je tomu jinak. U těchto požadavků kritéria ITSEC nepředepisují žádnou apriori danou množinu tříd bezpečnostní funkčnosti. Místo toho pouze definují zásady, jak takovou třídu bezpečnostní funkčnosti vytvořit. Pro usnadnění práce uživatelům kritérií a pro kompatibilitu s jinými kritérii jsou v příloze kritérií ITSEC uvedeny příklady tříd bezpečnostní funkčnosti. Pět z těchto tříd bezpečnostní 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 ekvivalentní třídám kritérií TCSEC.

Zbylých pět tříd bezpečnostní funkčnosti (F-IN, F-AV, F-DI, F-DC a F-DX) nemá hierarchickou strukturu. Tyto třídy bezpečnostní 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 zaručitelnosti bezpečnosti, 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 bezpečnostní 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 bezpečnostní funkčnosti, uvedených v kritériích ITSEC. Tato možnost dává uživateli kritérií větší možnosti a dovoluje mu vytvořit třídu bezpečnostní funkčnosti, která nejlépe odpovídá jeho požadavkům.

Třetí možností je, že uživatel kritérií použije některou, již vytvořenou třídu bezpečnostní funkčnosti, která není součástí kritérií ITSEC, ale je vytvořena v souladu s těmito kritérii a nejlépe vyhovuje požadavkům uživatele.

Konečně poslední, čtvrtou možností je případ, kdy si uživatel kritérií vytvoří sám vlastní třídu bezpečnostní 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.

2.1.2 Specifikace funkcí prosazujících bezpečnost podle ITSEC

Specifikace funkcí prosazujících bezpečnost (stanovení požadavků na bezpečnostní funkčnost) by měla být zpracována podle odstavců 2.18 až 2.64 kritérií ITSEC. V případě, že se uživatel kritérií rozhodne vytvořit si vlastní třídu funkčnosti, doporučuje se, aby použil systém generických záhlaví odstavců se specifikacemi, která jsou definována v kritériích ITSEC. Jedná se o následující generická záhlaví.

2.1.2.1 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.

2.1.2.2 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.

2.1.2.3 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.

2.1.2.4 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 trendové analýzy mohou také zahrnovat detekci potenciálních hrozeb bezpečnosti ještě předtím, než dojde k útoku. Některé funkce mohou splňovat požadavky na prokazatelnost přístupu 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.

2.1.2.5 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.

2.1.2.6 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.

2.1.2.7 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.

2.1.2.8 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): autentizace, řízení přístupu, důvěrnost dat, integrita dat, nepopiratelnost.

2.2 Bezpečnostní funkce podle kritérií CTCPEC

Kanadská kritéria pro hodnocení bezpečnosti informačních systémů CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) se pokusila 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 *účtovatel-*

nost. 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.

2.2.1 Bezpečnostní funkce zajišťující důvěrnost

Bezpečnostní funkce v této kategorii jsou určeny proti hrozbám, které mohou zapříčinit odhalení informace neoprávněným subjektům (neoprávněné prozrazení informace). Jedná se o následující bezpečnostní funkce:

- *Skryté kanály* (obsahuje čtyři úrovně CC-0 až CC-3)
  Tato bezpečnostní funkce se zabývá identifikací a odstraňováním takových toků informace, které jsou v rozporu s bezpečnostní politikou. Funkce se vyskytuje pouze v systémech s povinným řízením přístupu.
- *Nepovinné řízení důvěrnosti* (CD-0 až CD-4)
  Tato bezpečnostní funkce zahrnuje ty mechanismy nepovinného řízení přístupu k informacím (např. mechanismy přístupových práv, přístupové matice nebo seznamy přístupových práv), které přispívají k zajištění důvěrnosti dat.
- *Povinné řízení důvěrnosti* (CM-0 až CM-4)
  Tato bezpečnostní funkce zahrnuje ty mechanismy povinného řízení přístupu k informacím (např. mechanismy pracující se stupněm klasifikace spravovaných objektů), které přispívají k zajištění důvěrnosti dat.
- *Opětné použití objektů* (CR-0 až CR-1)
  Funkce opětné použití objektů zajišťuje, že objekt, přidělený uživateli nebo procesu neobsahuje žádné informace, zbylé od předchozího vlastníka objektu.

2.2.2 Bezpečnostní funkce zajišťující integritu

Bezpečnostní funkce v této kategorii jsou namířeny proti těm hrozbám, které představují neoprávněnou modifikaci (pozměnění) dat. Jedná se o následující bezpečnostní funkce:

- *Doménová integrita* (IB-0 až IB-2)
  Definuje tzv. důvěryhodnou výpočetní bázi (Trusted Computing Base, TCB) informačního systému a její schopnost ochránit se před útokem a spravovat chráněné objekty.
- *Nepovinné řízení integrity* (ID-0 až ID-4)
  Zahrnuje ty mechanismy nepovinného řízení přístupu k informacím (např. mechanismy přístupových práv, přístupové matice nebo seznamy přístupových práv), které přispívají k zajištění integrity dat.
- *Povinné řízení integrity* (IM-0 až IM-4)
  Zahrnuje ty mechanismy povinného řízení přístupu k informacím (např. mechanismy pracující se stupněm klasifikace spravovaných objektů), které přispívají k zajištění integrity dat.

- *Fyzická integrita* (IP-0 až IP-4)
  Definuje fyzický ochranný perimetr centralizované části systému a poskytuje služby pro ochranu komponent, které leží uvnitř tohoto perimetru.
- *Návrat* (IR-0 až IR-2)
  Zajišťuje schopnost produktu nebo systému IT vrátit se k předchozímu stavu po chybě uživatele, po havárii nebo po útoku.
- *Oddělení rolí* (IS-0 až IS-3)
  Oddělení rolí zajišťuje rozdělení pravomocí (např. přístupových práv) a zodpovědností mezi několik rolí a tím omezuje potenciální škody, způsobené nesprávným nebo nevhodným chováním uživatele nebo správce.
- *Autonomní testování* (IT-0 až IT-3)
  Tato funkce zahrnuje mechanismy, které slouží k testování, zda se hardware a software produktu nebo systému IT nachází ve správném a bezpečném stavu.

2.2.3 Bezpečnostní funkce zajišťující dostupnost

Bezpečnostní funkce zajišťující dostupnost mají za úkol zajistit, že uživatelům nemůže být neoprávněně odepřeno poskytnutí informací nebo služeb informačního systému. Jedná se o následující bezpečnostní funkce:

- *Přidělování prostředků* (AC-0 až AC-3)
  Kontroluje přidělování prostředků jednotlivým uživatelům a jejich využití uživateli.
- *Tolerance k chybám* (AF-0 až AF-23)
  Vlastnost systému, která vyjadřuje jeho schopnost umožnit výměnu vadných komponent bez přerušení poskytování služeb.
- *Robustnost* (AR-0 až AR-3)
  Vlastnost systému zajišťovat dostupnost informací a služeb i po výpadku některých komponent systému.
- *Zotavení* (AY-0 až AY-3)
  Umožňuje, aby se systém vrátil po poruše nebo chybě do známého a důvěryhodného stavu.

2.2.4 Bezpečnostní funkce zajišťující účtovatelnost

Tyto bezpečnostní funkce se týkají zodpovědnosti uživatelů za akce, které v systému provádějí. Jde o následující bezpečnostní funkce:

- *Audit* (WA-0 až WA-5)
  Zajišťuje detekci, zaznamenávání a pozdější analýzu událostí důležitých z hlediska bezpečnosti. Především zahrnuje tzv. mechanismus protokolování událostí.
- *Identifikace a autentizace* (WI-0 až WI-3)
  Zajišťuje zjištění a bezpečné ověření identity uživatele informačního systému.
- *Důvěryhodná cesta* (WT-0 až WT-3)
  Umožňuje uživateli bezpečnou a přímou komunikaci s centralizovaným informačním systémem.

2.3 Bezpečnostní funkce podle CC

V této kapitole 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*" [ISO/IEC 15408-2]. Výklad principů kritérií CC je náplní poslední kapitoly této příručky.

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 a/nebo pokrýt všechny identifikované bezpečnostní politiky organizace nebo jiné předpoklady.

Tato část ISO/IEC 15408 je určena spotřebitelům, vývojářům a hodnotitelům bezpečných systémů a produktů IT. Kapitola 3 dokumentu ISO/IEC 15408-1 poskytuje další informace o okruhu čtenářů ISO/IEC 15408 a o způsobu využití normy jednotlivými skupinami jeho čtenářů. Tyto skupiny mohou využít ISO/IEC 15408-2 následujícím způsobem:

- Zákazníci použijí ISO/IEC 15408-2 pří výběru komponent pro vyjádření svých funkčních požadavků, které splní bezpečnostní plán, vyjádřený PO nebo BC. Kapitola 4.3 dokumentu ISO/IEC 15408-1 poskytuje podrobnější informace o vztahu mezi bezpečnostním plánem a bezpečnostními požadavky.
- Vývojáři, kteří reagují na skutečné nebo předpokládané bezpečnostní požadavky spotřebitelů při vývoji produktu nebo systému IT, mohou v této části ISO/IEC 15408 nalézt normalizované metody pro porozumění požadavků zákazníků. Mohou také využít obsah této části ISO/IEC 15408 jako základ pro definici bezpečnostních funkcí a mechanismů, které splňují tyto požadavky.
- Hodnotitelé využijí funkční požadavky, definované v této části normy při ověřování, zda funkční požadavky, vyjádřené v PO nebo BC 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 normy na pomoc při rozhodování, zda daný produkt nebo systém IT splňuje dané požadavky.

2.3.1 Rozšiřování a údržba funkčních požadavků

Norma ISO/IEC 15408 a jeho 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/nebo *Bezpečnostní cíle* 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), jak je vysvětleno v přílohách B a C dokumentu ISO/IEC 15408-1.

2.3.2 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.

2.3.3 Model funkčních požadavků

Tato podkapitola popisuje model, použitý pro bezpečnostní funkční požadavky, uvedené v ISO/IEC 15408-2. Obrázky 2.1 a 2.2 zobrazují některé z klíčových konceptů modelu. Tato podkapitola obsahuje popisný text pro tyto obrázky a pro další klíčové koncepty, které nejsou na těchto obrázcích zobrazeny. Diskutované klíčové koncepty jsou zvýrazněny *kurzívou*.

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.

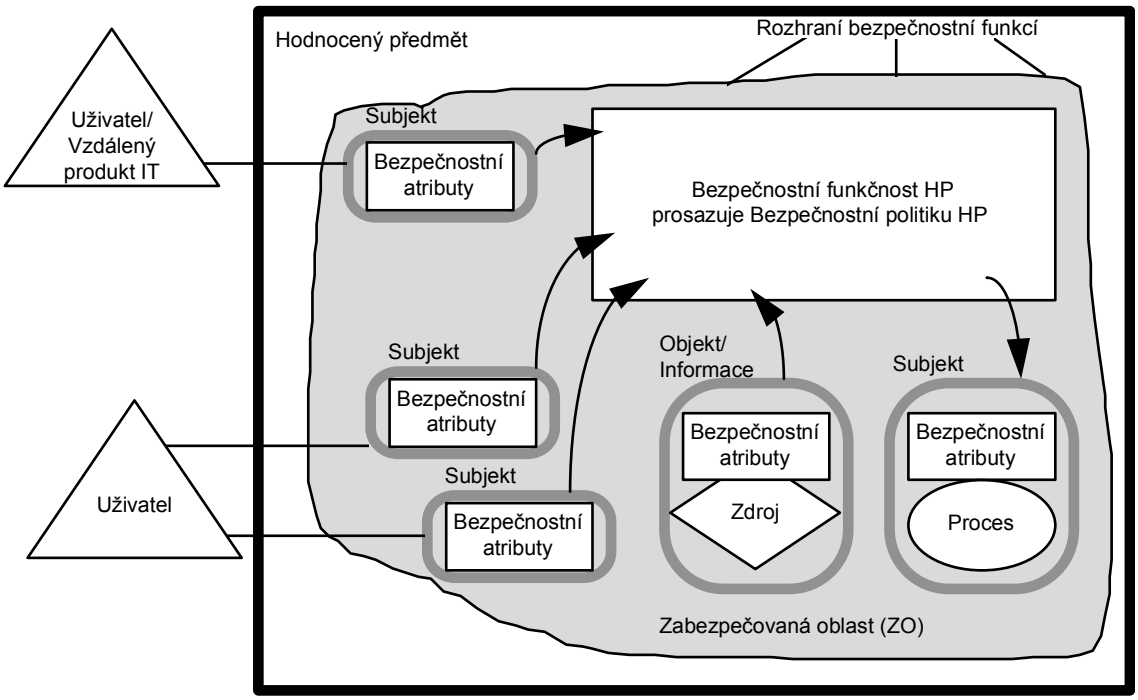
BPHP se skládá z několika *Bezpečnostních politik bezpečnostních funkcí (BPBF)*. Každá BPBF má svůj rozsah působnosti, který definuje subjekty, objekty a operace, řízené touto politikou. BPBF je implementována pomocí *Bezpečnostní funkce (BF)*, jejíž mechanismy prosazují politiku a poskytují k tomu nezbytné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

Monitor odkazů je abstraktní stroj, který prosazuje politiku řízení přístupu HP. *Mechanismus ověřování odkazů* je implementací principu monitoru odkazů, který splňuje následující vlastnosti: je odolný proti narušení, je vždy vyvolán a je dostatečně jednoduchý, aby mohl být předmětem detailní analýzy a testování. BPHP může sestávat z mechanismu ověřování odkazů a/nebo jiných bezpečnostních funkcí, nutných pro činnost HP.

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. 2.1 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:

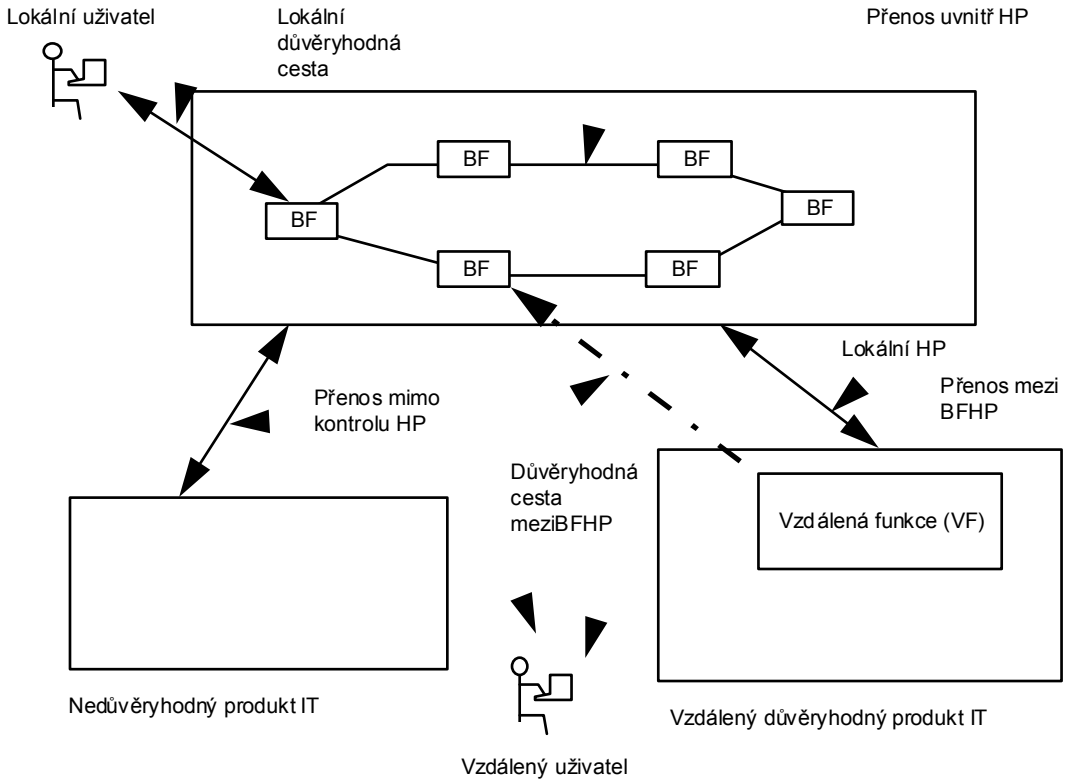
- Bezpečnostní politiky „vzdáleného důvěryhodného produktu IT“ a BP lokálního HP byly administrativně navzájem koordinovány a ohodnoceny. V tomto případě je výměna informací nazývána „*přenos mezi BFHP*“, jelikož k ní dochází mezi BFHP různých důvěryhodných produktů.
- Vzdálený produkt IT nemusí být ohodnocen, což je naznačeno na obr. 2.2 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. 2.2 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.

Pro vyjádření požadavků na oddělení pravomocí správce relevantní bezpečnostní funkční komponenty ISO/IEC 15408-2 (z rodiny komponent FMT_SMR) explicitně požadují *role* správců. Role je předdefinovaná sada pravidel, která určuje povolené interakce mezi uživatelem a HP. HP může podporovat definici libovolného počtu rolí. Např. role, týkající se bezpečného provozu HP, mohou být „správce auditu“ a „správce uživatelských účtů“.

HP obsahuje zdroje, které 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 ukládány.

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

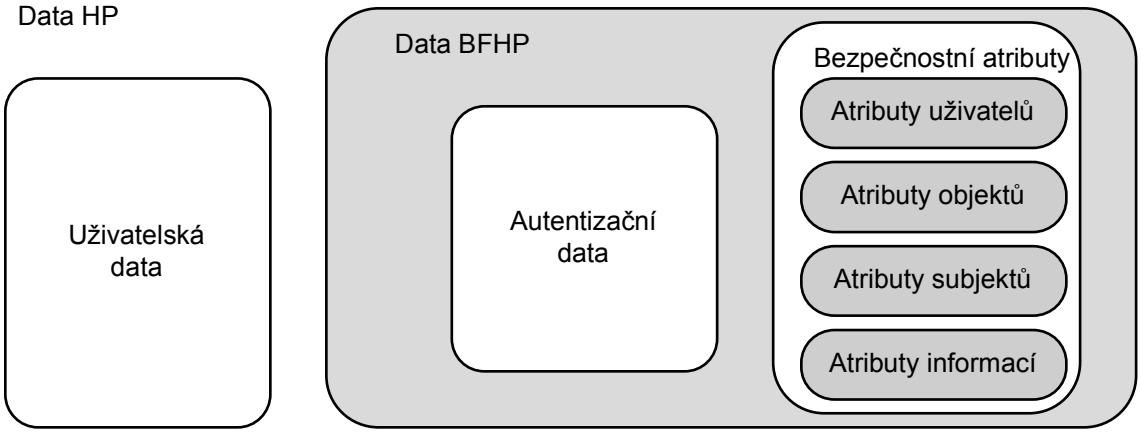
- Ty, které pracují pod kontrolou autorizovaného uživatele a které jsou subjektem všech pravidel BPHP (např. procesy v UNIXu).
- Ty, které pracují jako speciální funkční procesy, které mohou pracovat v zájmu mnoha uživatelů (např. funkce, které se nacházejí v architekturách klient/server).
- Ty, které 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 (např. meziprocesové komunikace), může subjekt vystupovat jako objekt. Objekty mohou obsahovat *informace*.

Uživatelé, subjekty, informace a objekty mají jisté *atributy*, které obsahují informace nutné k tomu, aby se HP choval správně. Některé atributy, jako jsou jména souborů, mohou být pouze informativní (tj. zvyšují uživatelskou přívětivost HP), zatímco jiné, jako jsou např. informace pro řízení přístupu, existují pouze za účelem prosazení BPHP. Tato druhá skupina atributů se nazývá "*bezpečnostní atributy*". Pokud není definováno jinak, je slovo atribut v ISO/IEC 15408 použito jako zkratka místo pojmu „bezpečnostní atribut". BPHP však může požadovat kontrolu nad všemi atributy, bez ohledu na to, jakého jsou typu.

Data uvnitř HP jsou kategorizována na dvě skupiny - uživatelská data nebo data BFHP. Obrázek 2.3 ukazuje jejich vztah. *Uživatelská data* jsou informace, uložené ve zdrojích HP, které mohou být uživateli zpracovávány v souladu s BPHP a kterým BFHP nepřisuzují žádný zvláštní význam. Např. obsah schránky elektronické pošty jsou uživatelská data. *Data BFHP* jsou informace, které používají BFHP pro provádění rozhodnutí podle BPHP. Pokud to BPHP dovolí, data BFHP mohou být ovlivněna (měněna) i uživateli. Příklady dat BFHP jsou bezpečnostní atributy, autentizační data a seznamy přístupových práv.



Obr. 2.3 Vztah mezi uživatelskými daty a daty BFHP

Některé BPBF se vztahují konkrétně na ochranu dat, jako např. *BPBF řízení přístupu* a *BPBF řízení toku dat*. Mechanismy, které implementují BPBF řízení přístupu, zakládají svá rozhodnutí na atributy subjektů, objektů a operací, které jsou pod kontrolou bezpečnostní politiky. Tyto atributy jsou použity v sadě pravidel, která řídí operace, jež mohou subjekty provádět na objektech. Mechanismy, které implementují BPBF řízení toku informace, zakládají svá rozhodnutí na atributech subjektů, kontrolovaných informacích a sadě pravidel, které řídí operace subjektů nad informacemi. Atributy informace, které mohou být sdruženy s atributy kontejneru

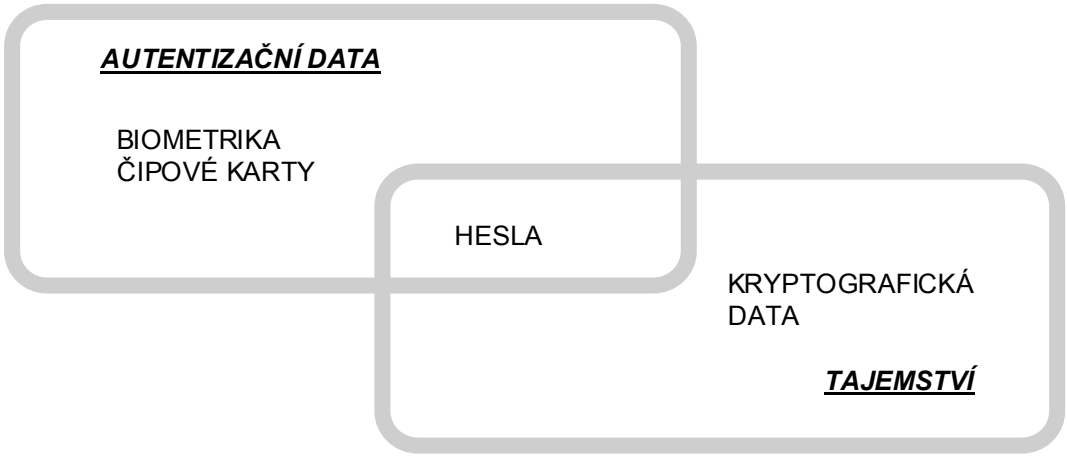
(nebo nemusí, jako v případě víceúrovňové databáze) se pohybují zároveň s pohybujícími se informacemi.

Dva specifické typy dat, které jsou uvedeny v ISO/IEC 15408-2, mohou, ale nemusí být totožné. Jde o *autentizační data* a *tajemství*.

Autentizační data se používají pro ověření identity uživatele, který požaduje služby od HP. Nejobvyklejší druh autentizačních dat je heslo, které musí být pro svou funkci účinného bezpečnostního mechanismu udrženo v tajnosti. Ne všechny formy autentizačních dat musí být tajné. Biometrická autentizační zařízení (např. snímače otisků prstů nebo snímače oční sítnice) nezávisí na utajení dat, ale na tom, že data představují něco, co má pouze jeden uživatel a co nemůže být paděláno.

Pojem tajemství, tak jak jej používají funkční požadavky ISO/IEC 15408-2, je sice aplikovatelný na autentizační data, ale je také aplikovatelný na jiné typy dat, která musí být udržena v tajnosti, aby byla prosazena konkrétní BPBF. Například mechanismus důvěryhodného kanálu, jehož schopnost udržet přenášené informace v tajnosti využívá kryptografie, je pouze tak silný, jak je silná metoda, použitá pro utajení kryptografických klíčů před neoprávněným odhalením.

Proto některá, ale nikoli všechna, autentizační data je třeba držet v tajnosti, a některá, ale ne všechna tajemství jsou použita jako autentizační data. Obrázek 2.4 ukazuje typická autentizační data a tajemství.



Obr. 2.4 Vztah mezi ”autentizačními daty” a ”tajemstvími”

2.3.4 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 (viz dále).

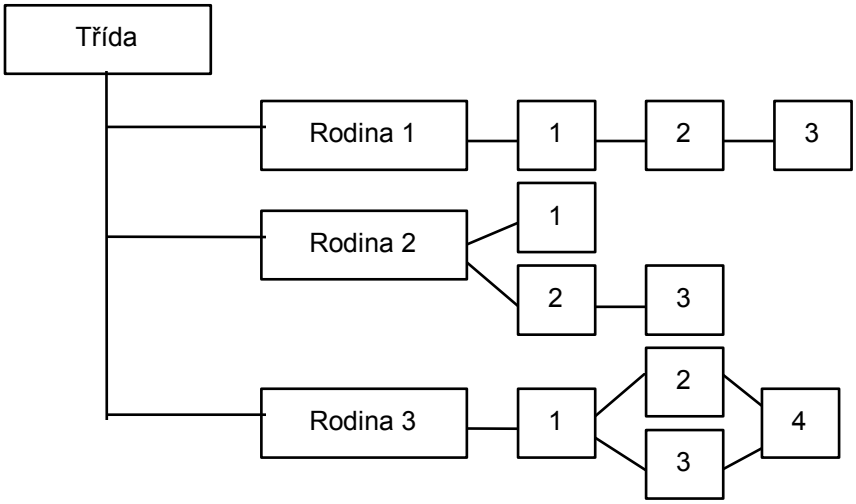
Katalog funkčních požadavků obsahuje třídy rodin a komponent, které jsou pouhým seskupením podle podobné funkce nebo podobného účelu a komponenty v rámci třídy jsou uvedeny v abecedním pořadí. Katalog obsahuje následující třídy:

- 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. 2.5.



Obr. 2.5 Ukázka rozdělení třídy na rodiny a komponent

Na obr. 2.5 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.

2.3.5 Třída FAU: Bezpečnostní audit

Bezpečnostní audit zahrnuje rozpoznávání, zaznamenávání, ukládání a analyzování informací, které mají vztah k aktivitám, významným z hlediska bezpečnosti (tj. aktivit, pokrytých 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

2.3.6 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

2.3.7 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 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

2.3.8 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 definovány 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.

2.3.9 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

2.3.10 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

2.3.11 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

2.3.12 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) k integritě 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. Kom-

ponenty 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, která 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

2.3.13 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

2.3.14 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

2.3.15 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

2.3.16 Minimální požadavky funkčnosti v návrhu bezpečnostního standardu SIS

V návrhu standardu bezpečnosti pro státní informační systém (publikace [BSSIS]) jsou v kapitole s názvem “Minimální programově technické požadavky” definovány funkční požadavky na (tehdejší) státní informační systém. Pro ilustraci požadované bezpečnostní funkce uvádíme v následujícím přehledu:

Identifikace a autentizace

- FIA-UID.1 Základní identifikace uživatele
- FIA-UAU.1 Základní autentizace uživatele
- FIA-ATD.1 Definice atributů uživatele
- FIA- ATA. Inicializace bezpečnostních atributů uživatele
- FIA- ADP.2 Rozšířená ochrana autentizačních dat uživatele

Audit

- FAU-GEN.1 Generování dat revize bezpečnosti
- FAU-GEN.2 Generování dat revize bezpečnosti s identitou uživatele
- FAU-STG.1 Stálé ukládání záznamů revize bezpečnosti
- FAU-PRO.1 Omezený přístup k záznamům revize bezpečnosti
- FAU-MGT.1 Správa záznamů revize bezpečnosti
- FAU-SEL.1 Selektivní revize bezpečnosti
- FAU-SEL.2 Run-timová selektivní revize bezpečnosti

Řízení přístupu

- FDP-ACC.1 Částečné řízení přístupu k objektům
- FDP-ACF.1 Řízení přístupu jednoduchými bezpečnostními atributy
- FDP-ACI.1 Statická inicializace atributů
- FDP-SAM.2 Modifikace bezpečnostních atributů uživatelem
- FDP -RIP.1 Částečná ochrana zbytkových informací na základě přidělení zdroje

Ochrana bezpečnostních funkcí hodnoceného předmětu

- FPT-TSA.1 Základní administrace bezpečnosti
- FPT-TSU.1 Prosazení vedení při administraci bezpečnosti
- FPT-SEP.1 Separace domén TSF
- FPT-RVM.1 Nemožnost obejít bezpečnostní politiku TOE
- FPT-AMT.1 Testování abstraktního počítače

Je třeba upozornit na to, že v době, kdy byl tento návrh standardu vytvářen, byla kritéria CC, ze kterých vychází funkční požadavky, ještě ve své předchozí verzi. V následující verzi (která byla vzata za základ normy ISO/IEC 15408) byla klasifikace bezpečnostních funkcí poněkud pozměněna, takže uvedené požadované bezpečnostní funkce nekorespondují s bezpečnostními funkcemi normy ISO/IEC 15408.

Číslice, uvedená za zkratkou komponenty (FPT-AMT.1), je pořadovým číslem komponenty v rodině bezpečnostních funkcí.

6. Hodnocení bezpečnosti

Cílem kapitoly je popsat filozofie, ze kterých vychází soudobé chápání bezpečnosti informačních technologií a jejího hodnocení mezinárodními normalizačními organizacemi, jmenovitě ISO/IEC. Porozumění těmto filozofiím umožní čtenáři porozumět jak normalizovaným principům hodnocení bezpečnosti produktů a systémů IT, které jsou určeny či zamýšleny k provozování ve třetím tisíciletí, tak i obecným principům jejich bezpečnosti.

6.1 Bezpečnost IT a kritéria bezpečnosti

Nacházíme se v éře, ve které ve stále větším počtu organizací lze považovat informace, uchovávané a zpracovávané informačními technologiemi, za zdroje kritické, tj. za zdroje, na kterých přímo závisí, zda daná organizace může plnit svoje poslání. Jednotlivci očekávají, že produkty nebo systémy IT zaručí adekvátní ochranu jejich soukromých (osobních) dat před neautorizovaným odhalením, neautorizovanou modifikací nebo před jejich ztrátou či dočasným znepřístupněním. Aby se tato ohrožení eliminovala, resp. aby se zajistilo zmírnění jejich vlivu, tj. aby se poskytla adekvátní ochrana, používá se soubor nástrojů (politiky, bezpečnostní funkce, bezpečnostní architektury) nazývaný bezpečnost IT.

Mají-li se používat IT bezpečně, je žádoucí mít k dispozici nějaký prostředek, který usnadní posouzení, zda daný produkt nebo systém IT je či není dostatečně bezpečný, resp. který usnadní vývoj produktů či systémů IT s bezpečností, která má předem zaručenou jistou *úroveň bezpečnosti*. V posledních dvou dekádách se postupně objevilo, používalo a používá několik takových nástrojů, vesměs nazývaných *kritéria bezpečnosti* (např. známá „oranžová kniha“ s kritérii amerického ministerstva obrany TCSEC nebo evropská „harmonizovaná“ kritéria ITSEC). V této kapitole se zabýváme hlavně výkladem kritérií bezpečnosti doporučovanými k používání jako základní metodický materiál pro hodnocení bezpečnostních vlastností produktů nebo systémů IT mezinárodní normou *ISO/IEC 15408*. Tato norma byla vydána teprve nedávno (v červnu r. 1999). Je výsledkem několikaleté mezinárodní iniciativy v rámci projektu pracovně nazývaném *Common Criteria for Information Technology Security Evaluation*. Z historických i pragmatických důvodů se proto v odborné veřejnosti i v uvedené normě pro tato kritéria i nadále používá označení *Common Criteria*, resp. zkratka *CC*.

6.2 Kritéria bezpečnosti ITSEC

Kritéria pro hodnocení bezpečnosti IT ITSEC (Information Technology Security Evaluation Criteria), ve slangu nazývaná "Superman Book", 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 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.

6.2.1 Rozsah kritérií ITSEC

Kritéria ITSEC lze aplikovat jak na produkt IT, tak i na systém IT. Jako produkt IT se chápe kupovaný produkt, který je prodáván pultovým prodejem bez znalosti konkrétního provozního prostředí, o jehož provozním prostředí lze vyslovit pouze obecné předpoklady. Systém IT je zasazen do konkrétního reálného provozního prostředí.

Sponzor hodnocení, entita, která požadavek na hodnocení zadává, určuje požadavky na provoz a hrozby. Dílčí bezpečnostní cíle hodnoceného předmětu dále závisí i na legislativních a dalších omezujících podmínkách. Tím se stanovuje požadovaná bezpečnostní funkcionalita a třída míry zaručitelnosti bezpečnosti (jinými slovy – úroveň důvěryhodnosti záruky za bezpečnost). Všechny aspekty hodnoceného předmětu, které jsou relevantní pro hodnocení, specifikuje bezpečnostní cíl. Popisuje bezpečnostní funkcionalitu hodnoceného předmětu, možné předpokládané hrozby, dílčí bezpečnostní cíle a detailní informace o použitých bezpečnostních mechanismech. Bezpečnostní cíl může obsahovat:

- dílčí bezpečnostní cíle (uvedené v celkové nebo v systémové bezpečnostní politice)
- definici provozního prostředí
- bezpečnostní funkce
- zdůvodnění použití bezpečnostních funkcí
- požadované bezpečnostní mechanismy a stanovení jejich minimální síly
- požadovanou třídu míry zaručitelnosti bezpečnosti.

Pro každou požadovanou třídu míry zaručitelnosti bezpečnosti kritéria definují, které podklady musí sponzor hodnocení hodnotiteli dodat. Hodnotitel převážně pracuje s podklady dodanými sponzorem hodnocení. Předpokládá se, že sponzor hodnocení a hodnotitel úzce spolupracují. Výsledkem procesu hodnocení je výrok, zda hodnocený předmět svůj bezpečnostní cíl splňuje či nesplňuje.

V kritériích ITSEC jsou požadavky na míru zaručitelnosti bezpečnosti a na bezpečnostní 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 zaručitelnosti bezpečnosti. 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 zaručitelnosti bezpečnosti. Pokud si uživatel zvolí určitou třídu podle požadavků na funkčnost, musí se smířit i s požadavky na míru zaručitelnosti bezpečnosti, 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 zaručitelnosti bezpečnosti.

Stanovení konkrétní třídy míry zaručitelnosti za bezpečnost podle kritérií ITSEC ovlivňuje proces vývoje hodnoceného předmětu, prostředí, ve kterém byl vyvíjen, úroveň jeho dokumentace a prostředí jeho provozu, proces dodávky, údržby apod. Sedm možných tříd zaručitelnosti bezpečnosti hodnoceného předmětu podle kritérií ITSEC lze stručně charakterizovat takto:

- E0 – nedostatečná zaručitelnost bezpečnosti, hodnocení nelze provést
- E1 – musí být dodán bezpečnostní cíl a neformální popis hodnoceného předmětu a testování bezpečnostních funkcí musí indikovat, že hodnocený předmět splňuje bezpečnostní cíl
- E2 – navíc proti E1 se požaduje dostupnost neformálního popisu detailního návrhu hodnoceného předmětu a hodnotiteli se musí dodat důkazy testování; musí se provádět správa konfigurace a musí být zaveden proces dodávky hodnoceného předmětu
- E3 – navíc proti E2 se požaduje dostupnost detailního návrhu a zdrojové texty programů bezpečnostních funkcí
- E4 – bezpečnostní politika hodnoceného předmětu musí být vyjádřena formálním modelem, požaduje se semiformální popis architektury a detailního návrhu hodnoceného předmětu a provedení analýzy zranitelnosti na této úrovni
- E5 – musí se prokázat úzká souvislost mezi detailním návrhem a implementací na úrovni zdrojových textů programů a provedení analýzy zranitelnosti na této úrovni
- E6 – požaduje se formální popis bezpečnostní architektury hodnoceného předmětu konzistentní s formálním modelem bezpečnostní politiky; musí být jednoznačně prokazatelná souvislost výkonných (binárních) programů s jejich zdrojovými formami.

Pro komerční bezpečné produkty je typickou třídou zaručitelnosti bezpečnosti třída E3.

6.2.2 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 popsán 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.

6.2.3 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".

6.2.3.1 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).

6.2.3.2 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.*

6.2.3.3 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.

6.3 Kritéria bezpečnosti CC

Zavedení obecné kriteriální základny pro hodnocení bezpečnosti IT umožňuje, aby výsledky hodnocení měly význam pro širší auditorium.

6.3.1 Čeho se CC týkají a čeho se netýkají

CC umožňují porovnávat výsledky nezávisle prováděných hodnocení bezpečnosti. Tohoto cíle dosahují tím, že stanovují obecně platné sestavy požadavků na:

- *bezpečnostní funkce* produktů a systémů IT
- *míry zaručitelnosti bezpečnosti* udělované (připisované) při hodnocení těmto bezpečnostním funkcím.

Proces hodnocení bezpečnosti IT prokazuje úroveň důvěryhodnosti, s jakou bezpečnostní funkce produktu nebo systému IT splňují stanovené požadavky. Stanovuje míru zaručitelnosti bezpečnosti udělované těmto bezpečnostním funkcím.

Kritéria CC definují hierarchicky uspořádané *úrovně zaručitelnosti bezpečnosti*. Množiny požadavků na splnění jednotlivých mír zaručitelnosti bezpečnosti, a tím pádem i míry zaručitelnosti bezpečnosti, jsou uspořádané do hierarchické soustavy podle těchto úrovní.

Výsledkem hodnocení je výrok o prokázání úrovně důvěryhodnosti, s jakou bezpečnostní funkce produktu nebo systému IT a míry zaručitelnosti bezpečnosti udělené těmto bezpečnostním funkcím splňují zavedené požadavky. Výrok sděluje, kterou úroveň zaručitelnosti bezpečnost produkt nebo systém IT splňuje.

Zákazník si může z výsledků hodnocení vybíraného nebo i již pořízeného produktu nebo systému IT odvodit, zda daný produkt nebo systém IT je pro zamýšlenou aplikaci dostatečně bezpečný, zda jsou rizika plynoucí z jeho provozování v konkrétních podmínkách tolerovatelná.

CC jsou užitečnou příručkou také pro vývojáře produktů nebo systémů IT, které mají být vybaveny bezpečnostní funkcionalitou, a také pro dodavatele takto funkčně vybavených komerčních produktů a systémů IT.

Produktem nebo systémem IT se rozumí např. operační systém, počítačová síť, databázový (distribuovaný) systém nebo nějaký jiný aplikační systém. Produkt nebo systém IT může obsahovat jak softwarové, tak i firmwarové nebo i hardwarové komponenty. CC označují hodnocený produkt nebo systém IT jako *hodnocený předmět*[27].

CC jsou cíleně orientována především na ochranu informací před neautorizovaným odhalením, neautorizovanou modifikací a před ztrátou možnosti s nimi pracovat. Obecně se tato hlediska označují jako ochrana důvěrnosti, ochrana integrity a ochrana dostupnosti informací. CC jsou primárně orientována na hrozby, jejichž zdrojem jsou především aktivity lidí (úmyslné nebo neúmyslné).

CC lze aplikovat i na další hlediska bezpečnosti a do dalších oblastí IT, autoři CC však nevyslovují žádné prohlášení o kompetentnosti CC mimo výše zmíněné domény použitelnosti.

CC se např. nezabývají hodnocením administrativních bezpečnostních opatření (organizační řády, personální politika, nástroje fyzické a procedurální ochrany apod.), pokud se tato opatření bezprostředně netýkají bezpečnostních opatření IT. Pokud tato opatření mají vliv na schopnost čelit identifikovaným hrozbám, považují se za bezpečná. Problému elektromagnetického vyzařování se CC věnují spíše okrajově. CC dále nedefinují žádné legislativní a organizační rámce pro své uplatňování. Předpokládá se, že komunita, která se jimi bude chtít řídit, si taková prostředí, tzv. s*chémata hodnocení bezpečnosti IT*, ustanoví. Prostředí pro uplatnění CC stanovuje odpovědné autority, jurisdikci, požadavky na vlastnosti akreditačních autorit, požadavky na vlastnosti hodnotitele apod.

Konečně je třeba upozornit i na skutečnost, že CC se záměrně nezabývají oceňováním kryptografických algoritmů. Předpokládá se, že pokud bude tato oceňování nějaká komunita požadovat, potřebná a vhodná legislativní opatření si zavede.

6.3.2 Pro koho jsou CC určena

Na hodnocení bezpečnostních vlastností produktů nebo systémů IT podle CC mají zájem tři skupiny – zákazníci, vývojáři a hodnotitelé produktů a systémů IT. CC jsou strukturována tak, aby uspokojila potřeby všech tří skupin. Všechny tři skupiny jsou chápány jako jejich primární uživatelé.

- *Zákazníci*

  Mohou použít CC při výběru požadavků na bezpečnost IT, kterými vyjadřují potřeby své organizace. CC jsou psána tak, aby zajistila, že hodnocení splní potřeby zákazníků (to je prvotním záměrem procesu hodnocení a ospravedlněním jeho provádění). Výsledek hodnocení mohou zákazníci použít při rozhodování, zda hodnocený produkt nebo systém IT splňuje jejich bezpečnostní potřeby.

  Bezpečnostní potřeby vesměs vyplynou z provedení analýzy rizik a z politických rozhodnutí. Zákazníci mohou výsledky hodnocení použít také pro porovnání různých produktů nebo systémů. Tuto potřebu podporuje hierarchie požadavků zaručitelnosti bezpečnosti.

  CC nabízejí zákazníkům, zvláště pak skupinám zákazníků a komunitám se shodnými zájmy, implementačně nezávislé struktury, nazývané *profily ochran*, ve kterých mohou vyslovovat své speciální požadavky na bezpečnostní opatření produktu nebo sytému IT.

[27] *TOE*, Target of Evaluation. Pro lepší čtivost textu budeme používat opis „produkt nebo systém IT“ nebo zkratku HP (hodnocený předmět).

- *Vývojáři*

  Použijí CC jednak pro přípravu hodnocení a jednak jako pomocný nástroj při hodnocení vyvíjeného produktu nebo systému IT a také jako návod pro identifikaci požadavků na bezpečnost, kterým musí vyvíjený produkt nebo systém IT vyhovět. Metodologie hodnocení, případně doplněná smlouvou o vzájemném uznávání výsledků hodnocení, umožňuje použít CC někým jiným než vývojářem pro hodnocení produktů nebo systémů IT používaných vývojářem.

  Vývojář může pomocí nástrojů zavedených v CC připravit důkazový (dokladový) materiál pro vyslovení tvrzení, že vyvinutý produkt nebo systém IT hodnocenými přesně stanovenými bezpečnostními funkcemi a zárukami bezpečnosti vyhovuje svým identifikovaným požadavkům. CC nabízejí pro vyjádření těchto požadavků na konkrétní vývojový případ implementačně nezávislou strukturu nazývanou *bezpečnostní cíl*. Požadavky široké zákaznické základny může podporovat jeden nebo několik profilů ochran.

  CC popisují bezpečnostní funkce, které vývojář může zahrnout do produktu nebo systému IT. CC lze použít pro určení odpovědností a činností při přípravě důkazových materiálů, které jsou požadovány pro hodnocení produktu nebo systému IT. CC rovněž definují obsah a formu prezentace důkazů.

- *Hodnotitelé*

  Mohou CC použít pro formulování posouzení, jak produkty nebo systémy IT vyhovují svým bezpečnostním požadavkům. CC popisují množinu činností, které hodnotitel musí provést a bezpečnostní funkce, kterých se tyto činnosti týkají. CC ale nespecifikují postupy při takovém hodnocení, tj. nedefinují v jakém pořadí a s jak formátovanými výstupy se činnosti hodnotitele provádí[28].

Mimo výše uvedené tři hlavní zájmové skupiny, jsou CC užitečná i pro manažery systémů IT a pracovníky oddělení bezpečnosti při vypracovávání bezpečnostních politik, pro auditory bezpečnosti IT a pro akreditační úředníky.

6.3.3 Jak lze hodnocení podle CC uplatnit

Aby byly výsledky hodnocení vzájemně porovnatelné, musí se provádět v rámci nějakého autoritativního prostředí – *schématu hodnocení bezpečnosti IT*, které stanoví normy (standardy), monitoruje kvalitu hodnocení a vydává předpisy, kterým musí hodnotící zařízení a hodnotitelé vyhovovat.

CC žádné takové předpisové prostředí nestanovuje. Nicméně, aby se dosáhlo kýženého cíle, tj. vzájemného uznávání výsledků hodnocení, musí být předpisová prostředí různých hodnotících autorit konzistentní. Kontext hodnocení produktů a systémů IT je tedy dán jednak kritérii CC a jednak následujícími prvky (viz obr. 6.1).

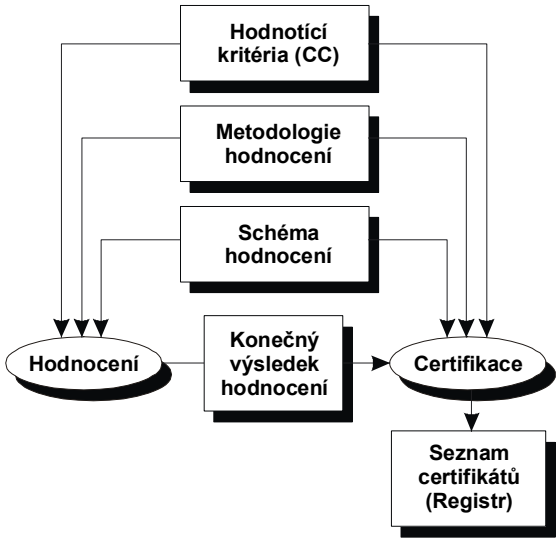
Jednotná obecná *metodologie hodnocení, která* sice přispívá k opakovatelnosti hodnocení a k objektivitě výsledků, ale sama o sobě není dostačující.

Mnohá hodnotící kritéria požadují použití expertních posudků, pro které je velmi obtížné dosáhnout konzistence. Aby se konzistentnost výsledků hodnocení zvýšila, měly by se konečné výsledky hodnocení podrobit *certifikačnímu procesu*. Certifikačním procesem se rozumí přezkoumávání výsledků hodnocení. Jedná se o prostředek pro zvýšení konzistence používání CC.

Certifikační proces končí vydáním konečného *certifikátu*, resp. schválení. Certifikát je normálně veřejně dostupný.

[28] Pro tento účel se připravuje norma, jejíž pracovní verze je známá pod *názvem Common Methodology for IT Security Evaluation, CME*.

Za schéma hodnocení bezpečnosti IT, metodologii hodnocení a certifikační proces včetně certifikátu jsou odpovědné autority hodnocení pověřené provozováním schémat a CC se jimi nezabývají.



Obr.6.1 Kontext hodnocení

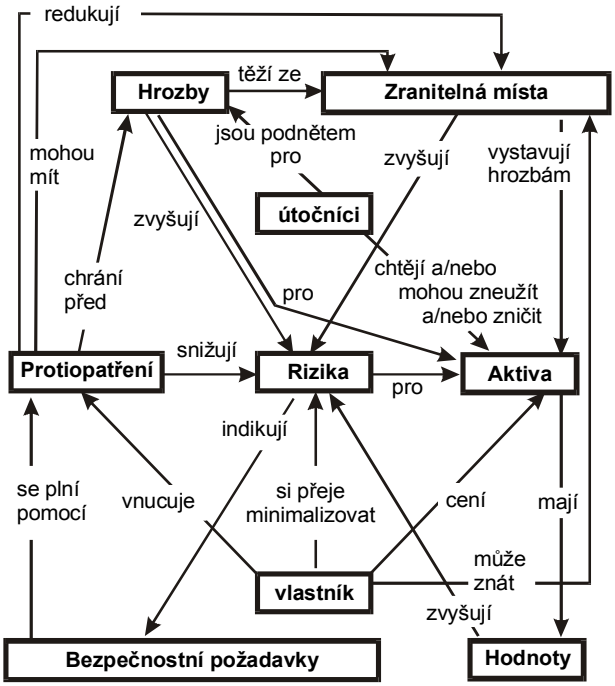
6.4 Model bezpečnosti CC

Základní pojmy z oblasti bezpečnosti a vztahy mezi nimi uvádí obr. 6.2. *Bezpečnost* se zabývá ochranou *aktiv* před *hrozbami*. Hrozby představují možnost neoprávněného využitkování aktiv. CC se zaměřují především na hrozby plynoucí z lidských zlomyslných nebo neúmyslných aktivit. Za chránění aktiva je odpovědný jeho vlastník, který aktivu přisuzuje hodnotu. Aktiva mohou mít hodnotu i pro skutečného nebo domnělého útočníka, který se proto snaží aktiva využitkovat způsobem, který odporuje zájmům vlastníka aktiva. Vlastník vnímá takové hrozby jako potenciální škodu, která snižuje hodnotu jeho aktiv.

Mezi základní typy hrozeb CC řadí ztrátu *důvěrnosti* (důvěrné aktivum se odhalí neoprávněnému příjemci), ztrátu *integrity* (aktivum je neoprávněně modifikováno) a ztrátu *dostupnosti* (způsobenou neoprávněným omezením přístupu k aktivu).

Vlastník aktiv analyzuje hrozby, kterým jsou jeho aktiva vystavena, vyhodnocuje, s jakými pravděpodobnostmi a s jakými typy útoků musí počítat, určuje *rizika*. Zná-li vlastník aktiva potenciální škodu a rizika, volí *bezpečnostní opatření*, kterými bude rizikům čelit a snižovat je na přijatelnou mez. Opatření se zavádějí tak, aby redukovala zranitelnost příslušného produktu nebo systému IT a aby se plnila bezpečnostní politika vlastníka aktiv. Zbytková rizika se vlastníci aktiv snaží minimalizovat dalšími omezeními, která nemusí být nutně z oblasti IT.

Vlastníci aktiv potřebují důvěřovat, že uplatněná bezpečnostní opatření adekvátně čelí hrozbám jejich aktiv, a to ještě dříve, než tato aktiva konkrétním hrozbám vystaví. Vlastníci aktiv nemusí být schopni sami posoudit všechna hlediska důvěryhodnosti přijatých bezpečnostních opatření a mohou si přijetí opatření nechat zhodnotit. Výstupem takového hodnocení je výrok, který charakterizuje, do jaké míry lze dát záruku za to, že přijatým bezpečnostním opatřením lze důvěřovat z hlediska kýžené minimalizace rizik. Hodnocení musí být objektivní a musí poskytovat opakovatelné výsledky, které lze v dalších hodnoceních citovat jako důkazový materiál.



Obr. 6.2 Základní bezpečnostní pojmy a vztahy mezi nimi

6.5 Pojetí bezpečnosti podle CC

Proces stanovení požadavků na bezpečnost produktu nebo systému IT musí bezpodmínečně vycházet z kontextu jeho použití a jeho obsahu. Bezpečný produkt nebo systém IT bývá provozován v nějakém prostředí, měl by vyhovovat nějakému profilu ochrany nebo bezpečnostnímu cíli.

6.5.1 Prostředí produktu nebo systému IT

Všechny relevantní zákonné a právní normy, bezpečnostní politiky organizace, zákazníci, odbornost a znalosti související se zabezpečovaným produktem nebo systémem IT vytvářejí *prostředí zabezpečovaného produktu nebo systému IT*. Toto prostředí definuje kontext, ve kterém se má produkt nebo systém IT používat. Do zabezpečovaného prostředí patří také hrozby pro bezpečnost IT, které v něm existují nebo by v něm mohly existovat.

Ten, kdo připravuje profil ochrany nebo bezpečnostní cíl související s jistým typem prostředí, musí brát do úvahy konkrétní typ fyzického prostředí, ve kterém se budou odpovídající produkty nebo systémy IT provozovat, známé principy fyzické a personální bezpečnosti, typy aktiv, která se mají chránit, a to jak přímých aktiv (soubory, databáze), tak i nepřímých, odvozených aktiv (certifikáty, autorizační pověření, vlastní implementaci IT) a účel, proč se mají produkty nebo systémy IT používat. Z hlediska potřeb pro definici profilů ochran a bezpečnostních cílů je nutné vypracovat:

- výčet předpokladů, které musí prostředí produktu nebo systému IT splnit, aby ho bylo možné považovat za bezpečné
- výčet hrozeb, které se považují v daném prostředí za relevantní (předpokládané metody útoku, zranitelná místa využitelná k útoku, ohrožená aktiva); ocenění bezpečnostních rizik by mělo vymezit pro každou hrozbu pravděpodobnost, se kterou se hrozba uplatní, pravděpodobnost úspěchu takového útoku a důsledky případných škod
- vyjádření bezpečnostních politik organizace, které bude možno v produktu nebo systému IT citovat a považovat je platné.

6.5.2 Bezpečnostní plán

Výsledek analýzy prostředí zabezpečovaného produktu nebo systému IT lze posléze použit pro definici *bezpečnostních plánů*, kterými se čelí identifikovaným hrozbám, které oslovují identifikované bezpečnostní politiky organizace a předpoklady. Bezpečnostní plány mají být konzistentní s definovanými provozními úmysly, se zamýšlenými účely produktu a se všemi znalostmi o fyzickém prostředí. Účelem vypracování bezpečnostního plánu je určit všechny bezpečnostní problémy a deklarovat, která bezpečnostní hlediska jsou dána přímo produktem nebo systémem IT a která jeho prostředím. Tato kategorizace je založena na procesu zahrnování konstrukčních úvah, bezpečnostních politik, ekonomických hledisek a rozhodnutí o přijatelnosti zbytkových rizik. Bezpečnostní plány pro dané prostředí by měly být implementovatelné pomocí IT, ale mohou se implementovat i netechnickými nebo i procedurálními (organizačními) prostředky. Na bezpečnostní plány se odkazuje při stanovování požadavků na bezpečnost IT.

6.5.3 Požadavky na bezpečnost IT

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.

6.5.4 Profil ochrany a bezpečnostní cíl

CC definují tři typy sestav požadavků na bezpečnost, jednu pomocnou a dvě cílové:

- *balík* (package)
  Je základní stavební jednotka pro skladbu jednotlivých požadavků do dílčích celků, na balík lze klást jak funkční požadavky, tak i požadavky zaručitelnosti bezpečnosti, z balíků se konstruují větší balíky, profily ochran, resp. bezpečnostní cíle.
- *profil ochrany* (protection profile)
  Umožňuje implementačně nezávisle stanovit požadovanou cílovou úroveň zaručitelnosti bezpečnosti a bezpečnostní funkcionalitu pro skupinu produktů nebo systémů IT, které budou plně vyhovovat dané množině bezpečnostních plánů;
  profily ochran se stanovují jako opakovaně použitelné a definují požadavky na produkt nebo systém IT, o kterých se ví, že jsou užitečné a potřebné pro splnění daných bezpečnostních plánů;
  profily ochran obsahují i logická zdůvodnění bezpečnostních plánů a bezpečnostních požadavků;
  profily ochran by mohly vypracovávat komunity uživatelů, vývojářů a jiných stran se společnými (příbuznými, shodnými) zájmy na bezpečnosti; na profily ochran se lze odkazovat při definování konkrétních bezpečnostních potřeb.
- *bezpečnostní cíl*
  Je určen pro vyjádření bezpečnostních požadavků na konkrétní produkt nebo systém IT;
  bezpečnostní cíl obsahuje množinu bezpečnostních požadavků, které lze zavést citováním některého profilu ochrany, případně přímým citováním odkazu na bezpečnostní komponentu nebo na komponentu zaručitelnosti za bezpečnost nebo explicitním vypracováním;
  bezpečnostní cíl dále obsahuje přehled specifikací produktu nebo systému IT, zadaných bezpečnostních požadavků a cílů a jejich logická zdůvodnění.

6.6 Bezpečnostní funkcionalita produktu/systému IT

Hlubší rozbor bezpečnostní funkcionality zaváděné v CC přesahuje rámec této kapitoly, který si klade za cíl seznámit čtenáře se základními filozofiemi a přístupy nově zaváděné normy ISO/IEC 15408. Systematickým rozborem bezpečnostních funkcí se zabývala kapitola 3. V pestrosti bezpečnostní funkcionality CC nepřinášejí žádné zásadní převratné změny proti chápání bezpečnostní funkcionality na konci 90. let. Omezíme se proto jen na orientační výčet bezpečnostní funkcionality považované v CC za standardní nástroje ochrany.

CC zavádějí bezpečnostní funkce v pojmech třída, rodina a komponenta. Každá *funkční třída* obsahuje (mimo definici své identity a popisu své struktury a účelu) alespoň jednu funkční rodinu, každá funkční rodina sestává z alespoň jedné funkční komponenty. Funkční komponenta je dále nedělitelný bezpečnostní element bezpečnostní funkcionality. Tak např. funkční třída *Identifikace a autentizace* sestává z funkčních rodin řešících dílčí bezpečnostní problémy typu *Definice atributů uživatelů*, *Specifikace tajemství*, *Autentizace uživatele*, *Identifikace uživatele* apod. Dále pak např. rodina *Autentizace uživatele* obsahuje pro plnění svého účelu komponenty (elementární bezpečnostní funkce) typu *Práce s časem*, *Jednorázová autentizace*, *Násobná autentizace* atd. Mezi standardní třídy bezpečnostních funkcí CC zahrnují bezpečnostní audit, komunikaci, kryptografickou podporu, ochranu dat uživatele, identifikaci a autentizaci, správu bezpečnosti, ochranu soukromí, ochranu bezpečnostní funkcionality, ochranu dostupnosti zdrojů, přístup k produktu nebo systému IT a důvěryhodné kanály a cesty.

6.7 Požadavky zaručitelnosti bezpečnosti

Cílem této kapitoly je popsat filozofii, ze které vychází přístup normy ISO/IEC 15408 k chápání zaručitelnosti bezpečnosti produktů a systémů IT.

6.7.1 Paradigma zaručitelnosti bezpečnosti IT

6.7.1.1 Základní filozofie zaručitelnosti bezpečnosti IT

Hrozby z hlediska bezpečnosti a z hlediska plnění požadavků daných bezpečnostní politikou organizace se mají vyslovovat jasně (tj. zřetelně a srozumitelně) a navrhovaná bezpečnostní opatření mají být z hlediska jejich zamýšleného účelu prokazatelně (tedy jasně, evidentně) dostatečná. Je nutné zavádět opatření, která snižují:

- pravděpodobnost existence zranitelných míst
- schopnost využití zranitelného místa (tj. záměrným využitkováním nebo neúmyslným podnětem)
- rozsah škod, které by mohly vzniknout využitím zranitelného místa.

Dále se mají zavádět opatření, která usnadňují:

- pozdější identifikaci zranitelných míst
- odstraňování škod, zmírňování následků a/nebo oznamování, že nějaké zranitelné místo bylo využitkováno nebo v něm neúmyslně vznikl podnět k jeho využití.

6.7.1.2 Role hodnocení

Zaručitelnost bezpečnosti jistého produktu nebo systému IT odvozuje z výsledků získaných hodnocením (tj. aktivním vyšetřováním) produktu nebo systému IT, který má být důvěryhodný. Hodnocení je tradiční prostředek pro poskytnutí záruky, je základem jak dokumentů dosud používaných hodnotících kritérií, tak i dokumentů ISO/IEC 15408. Norma ISO/IEC 15408 navrhuje provádět posuzování platnosti dokumentace a výsledného produktu nebo systému IT zkušenými hodnotiteli. Velký důraz se klade na rozsah, hloubku a přísnost hodnocení. Norma ISO/IEC 15408 nepopírá vynikající vlastnosti jiných nástrojů pro odvození zaručitelnosti bezpečnosti v IT, ani je nekomentuje. Ve výzkumu alternativních cest k získání zaručitelnosti bezpečnosti se pokračuje a norma ISO/IEC 15408 je strukturována tak, že nic nebrání tomu, aby je později akceptovala.

6.7.1.3 Ošetření zranitelných míst

Předpokládá se, že existují útočníci, kteří budou aktivně vyhledávat, jak využitkovat příležitosti k porušení bezpečnostních politik. Jejich motivací je snaha dostat se k nedovolenému výtěžku využitkováním aktiv. Útočníkem může být i ten, kdo provádí sice dobře myšlené, ale nicméně nebezpečné akce. Útočníci také mohou dávat podnět k využití zranitelných míst neúmyslně, a organizaci tak způsobovat újmu nechtěně.

Protože zpracovávání citlivých informací se nelze vyhnout a adekvátně důvěryhodné produkty a systémy IT dosud nejsou dostatečně dostupné, poruchy v IT jsou příčinou vysokých rizik. Je tudíž pravděpodobné, že prolomení bezpečnosti IT může vést k závažným ztrátám pro organizaci.

Prolomení bezpečnosti IT vzniká záměrným využitkováním zranitelných míst nebo neúmyslným podnětem k jejich využití v aplikaci IT provozované v nějakém reálném prostředí (obchodní činnosti apod.). Je proto žádoucí vykonat potřebné kroky s cílem prevence vzniku zranitelných míst v produktech a systémech IT. Zranitelná místa mají být v proveditelné míře:

- *odstraněna*
  tj. mají být vykonány aktivní kroky vedoucí k odhalení a k odstranění nebo k neutralizování všech využitelných zranitelných míst, nebo
- *minimalizována*
  tj. mají být vykonány aktivní kroky vedoucí k omezení potenciálního dopadu využití zranitelného místa na akceptovatelnou zbytkovou úroveň, nebo
- *monitorována*
  tj. mají být vykonány aktivní kroky vedoucí k zajištění, že jakýkoliv pokus o využití zbytkového zranitelného místa bude detekován, což umožní následně provést kroky minimalizující škodu.

6.7.1.4 Vznik zranitelných míst

Zranitelná místa vznikají jako důsledek selhání (opomenutí, zanedbání):

- ve specifikaci požadavků
  produkt nebo systém IT může plnit všechny funkce a vykazovat všechny rysy po něm požadované a přesto stále ještě obsahuje zranitelná místa, která ho činí z hlediska bezpečnosti nevhodným nebo neúčinným
- v konstrukci
  produkt nebo systém IT nesplňuje svoje specifikace a/nebo byla do něj zavlečena zranitelná místa v důsledku špatných konstrukčních standardů nebo nesprávných rozhodnutí (voleb) při jeho návrhu
- v provozu,
  produkt nebo systém IT byl sice správně zkonstruován podle správných specifikací, ale zranitelná místa do něj byla zavlečena v důsledku použití neadekvátních provozních řídicích nástrojů.

6.7.2 Zaručitelnost bezpečnosti IT podle CC

Zaručitelností bezpečnosti IT se rozumí důvody, příčiny, motivy a pohnutky opravňující důvěřovat, že produkt nebo systém IT splňuje své bezpečnostní plány. Zaručitelnost bezpečnosti IT lze odvodit z odkazů na takové zdroje, jako jsou nepodložená tvrzení, předchozí relevantní zkušenost nebo specifická zkušenost. Norma ISO/IEC 15408 ale odvozuje zaručitelnost bezpečnosti aktivním vyšetřováním. Aktivním vyšetřováním se rozumí hodnocení produktu nebo systému IT s cílem přesně určit jeho bezpečnostní vlastnosti.

6.7.2.1 Zaručitelnost bezpečnosti je odvozená z výsledků hodnocení

Tradičním prostředkem pro získání zaručitelnosti bezpečnosti je hodnocení a hodnocení je i základem přístupu k vyslovení zaručitelnosti bezpečnosti podle normy ISO/IEC 15408. Mezi hodnotící techniky lze zahrnout (bez nároku na úplnost výčtu):

- analýzu a kontrolu procesu (procesů) a procedury (procedur)
- kontrolu, že se proces(y) a procedura(y) používají
- analýzu korespondence mezi reprezentacemi návrhu hodnoceného předmětu (produktu nebo systému IT)
- analýzu reprezentace návrhu hodnoceného předmětu (produktu nebo systému IT) proti zadaným požadavkům
- ověřování (verifikace) důkazů
- analýzu dokumentů s návody, příruček
- analýzu vyvinutých testů funkcí a poskytnutých výsledků testů
- nezávislé testování funkcí (třetí stranou)
- analýzu zranitelných míst (včetně hypotéz o selháních)
- testování možností průniků.

6.7.2.2 Škálování zaručitelnosti bezpečnosti plynoucí z hodnocení

Filozofie normy ISO/IEC 15408 prosazuje dvě zásady:

- z vynaložení většího hodnotícího úsilí plyne důvěryhodnější zaručitelnost bezpečnosti
- cílem je vynakládat minimální hodnotící úsilí požadované pro poskytnutí nutné úrovně zaručitelnosti bezpečnosti.

Zvyšování úrovně hodnotícího úsilí se opírá o:

- *rozsah hodnocení*
  úsilí je větší, když se do hodnocení zahrnuje větší část produktu nebo systému IT
- *hloubku hodnocení*
  úsilí je větší, když je hodnocení rozvíjeno na jemnějších úrovních návrhu a na jemnějších implementačních detailech
- *přísnost hodnocení*
  úsilí je větší, když se hodnocení provádí strukturovanějším, formálnějším stylem.

6.7.2.3 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.

6.7.3 Klasifikace požadavků zaručitelnosti bezpečnosti

Aby bylo možné používat nějakou taxonometrii při klasifikaci požadavků zaručitelnosti bezpečnosti, zavádějí se kategorie třída požadavků zaručitelnosti bezpečnosti (abstraktnější pohled) a rodina požadavků zaručitelnosti bezpečnosti (detailnější pohled).

6.7.3.1 Třída a rodina požadavků zaručitelnosti bezpečnosti

Nejobecněji chápaná sestava požadavků zaručitelnosti bezpečnosti pokrývá jistou problémovou oblast a nazývá se *třída*. Každá třída požadavků zaručitelnosti bezpečnosti sestává z jedné nebo několika *rodin*. Rodina požadavků zaručitelnosti bezpečnosti charakterizuje podmínky pro zaručitelnost bezpečnosti v některé dílčí problémové oblasti.

Definice třídy požadavků zaručitelnosti bezpečnosti třídu pojmenovává, popisuje záměr jejího zavedení a její strukturu. Definice rodiny požadavků zaručitelnosti bezpečnosti rovněž rodinu pojmenovává, dále pak uvádí obecné bezpečnostní cíle, které zavedení rodiny sleduje a popisuje její strukturu tvořenou z jednotlivých komponent zaručitelnosti bezpečnosti; v definici rodiny požadavků zaručitelnosti bezpečnosti se zavedení hierarchie komponent zdůvodňuje a vymezuje se rozsah, hloubka a přísnost jejich hodnocení.

6.7.3.2 Příklady tříd a rodin požadavků zaručitelnosti bezpečnosti

Jako příklady tříd požadavků zaručitelnosti bezpečnosti a jejich rodin lze uvést následující příklady tříd vymezené těmito problémovými oblastmi:

- správa konfigurace
  - automatizace správy konfigurace – definují se úrovně automatizace
  - schopnosti správy konfigurace – definují se charakteristiky systému správy
  - oblast správy konfigurace – uvádějí se položky produktu nebo systému IT řízené systémem správy konfigurace
- dodávka a provoz
  - dodávka – procedury použité pro udržování bezpečnosti během dodávky produktu nebo systému IT uživateli (počáteční i udržovací, záruka autenticity produktu nebo systému IT apod.)
  - instalace, generování a spuštění produktu nebo systému IT, nastavení jeho bezpečnostní funkcionality
- vývoj
  - specifikace bezpečnostní funkcionality
  - návrh na vysoké úrovni abstrakce – základní struktury bezpečnostní funkcionality, hlavní softwarové, hardwarové a firmwarové prvky
  - reprezentace implementace – zdrojové kódy, hardwarová schémata
  - návrh na nízké úrovni abstrakce (detailní návrh) – základ pro programování a konstrukci hardwaru
  - model bezpečnostní politiky – modely zvyšují záruku, že funkční specifikace odpovídá bezpečnostní politice
- dokumentace s návody
  - dokumentace správce
  - dokumentace uživatele

- podpora životního cyklu
  - bezpečnost vývoje – fyzické, procedurální, personální bezpečnostní opatření použitá ve vývojovém prostředí
  - oprava vad
  - konstrukční postupy použité při vývoji produktu nebo systému IT
  - vývojové nástroje a techniky
- testy
  - pokrytí – stanovení, které bezpečnostní funkce se testují
  - hloubka – detailnost, granularita, na které vývojář testoval produkt nebo systém IT
  - testy prováděné vývojářem
  - testy prováděné nezávislou autoritou (třetí stranou)
- oceňování zranitelnosti
  - analýza skrytých kanálů
  - analýza možnosti nesprávného použití – lze rozpoznat, že systém není bezpečně konfigurován a provozován
  - analýza síly bezpečnostních funkcí – např. analýza mechanismu hesel
  - analýza zranitelnosti – identifikace vad zavlečených při vývoji (úplnost bezpečnostní funkcionality, závislosti mezi bezpečnostními funkcemi), testování možností průniků

6.7.4 Specifikace požadavků zaručitelnosti bezpečnosti

Rodina požadavků zaručitelnosti bezpečnosti sestává z jedné nebo více *komponent*, každá komponenta podmínka sestává z jednoho nebo více *prvků*. Komponenty a prvky se používají pro specifikaci požadavků zaručitelnosti bezpečnosti v profilech ochrany[29] nebo v bezpečnostních cílech[30].

6.7.4.1 Komponenty a prvky zaručitelnosti bezpečnosti

Každá *komponenta zaručitelnosti bezpečnosti* je identifikována, kategorizována, registrována a odkazována pomocí své identifikace. Její definice dále uvádí přesně stanovené bezpečnostní cíle, záměry a detailní popis těchto cílů a záměrů, případné aplikační poznámky, které usnadňují jejich použití, a nakonec uvádí popis souvislostí mezi komponentami a definuje prvky tvořící danou komponentu rodiny požadavků. *Prvek zaručitelnosti bezpečnosti* představuje takový elementární bezpečnostní požadavek, který by po dalším dělení neposkytnul smysluplný hodnotitelný výsledek. Představuje tudíž nejmenší samostatný bezpečnostní požadavek. Každý prvek zaručitelnosti bezpečnosti se řadí do jedné ze tří skupin:

- *prvky vývojových akcí*
  činnosti, které má vývojář dělat a vymezení důkazových materiálů popsaných v následující skupině
- *důkazové prvky*
  požadované důkazy, popis co má důkaz demonstrovat, jakou informací má důkaz vyjádřit

[29] implementačně nezávislá soustava bezpečnostních požadavků na jistou kategorii produktů nebo systémů IT, která splňuje určité, přesně stanovené potřeby zákazníka

[30] množina bezpečnostních požadavků a specifikací používaná jako základ pro hodnocení/definování bezpečnosti produktu nebo systému IT

- *hodnotitelské akce*
  činnosti, které má provádět hodnotitel. Explicitně mezi takové akce patří potvrzení, že jsou splněny požadavky popsané pomocí důkazových prvků. Dále sem patří akce a analýzy, které by měl provádět hodnotitel jako dodatečná hodnocení k akcím, které již byly provedeny vývojářem. Pokud nejsou výsledky některých akcí vývojáře pokryty důkazovými prvky, musí odpovídající akce implicitně provést hodnotitel.

Akce vývojáře a důkazový materiál definují ty požadavky zaručitelnosti bezpečnosti, které jsou posléze použity pro vyjádření odpovědnosti vývojáře při prokazování zaručitelnosti v bezpečnostní funkcionalitě hodnoceného produktu nebo systému IT. Pokud vývojář tyto podmínky zaručitelnosti bezpečnosti splní, může mít vyšší důvěru v to, že jeho produkt nebo systém IT vyhovuje funkčním požadavkům a požadavkům zaručitelnosti bezpečnosti stanoveným profilem ochrany nebo bezpečnostním cílem.

Akce hodnotitele definují odpovědnost hodnotitele ve dvou rovinách. Hodnotitel jednak ověřuje a potvrzuje, že jsou splněny dané bezpečnostní cíle, resp. že hodnocený produkt nebo systém IT vyhovuje danému profilu ochrany, a jednak ověřuje, že hodnocený produkt nebo systém IT odpovídá stanoveným požadavkům na funkčnost a stanoveným požadavkům zaručitelnosti bezpečnosti. Když hodnotitel prokáže, že je správně implementován profil ochrany, resp., že jsou splněny bezpečnostní cíle a požadavky zaručitelnosti bezpečnosti, může poskytnout podklad pro oprávněnost důvěry v to, že hodnocený produkt nebo systém IT splňuje své bezpečnostní plány. Prvky vývojových akcí, důkazové prvky a požadavky stanovující explicitní akce hodnotitele identifikují úsilí hodnotitele, které má vynaložit při ověřování tvrzení o bezpečnosti, která jsou uvedena jako bezpečnostní cíle v hodnoceném produktu nebo systému IT.

Prvky zaručitelnosti bezpečnosti reprezentují požadavky, které se musí splnit. Vyjadřují se jasně, stručně a jednoznačně. Žádné složené věty, každá samostatná podmínka se vyjadřuje jako jeden prvek zaručitelnosti. Spíše než zkratkovitá symbolická vyjádření pomocí omezených množin rezervovaných pojmů se používá přirozeného jazyka.

6.8 Charakteristiky úrovní zaručitelnosti bezpečnosti

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

6.8.1 EAL1, funkčně testovaný produkt nebo systém IT

6.8.1.1 Cíle EAL1

- 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.

6.8.1.2 Záruky EAL1

- Úroveň EAL1 je základní úrovní zaručitelnosti bezpečnosti danou výsledky analýzy bezpečnostních funkcí pomocí specifikací funkcí a rozhraní a dokumentace s návody prováděnou s cílem porozumět bezpečnostnímu chování.
- Analýza se podporuje nezávislým testováním bezpečnostních funkcí.
- Ve srovnání s nehodnocenými produkty nebo systémy IT úroveň EAL1 představuje významně vyšší zaručitelnost bezpečnosti.
- Hodnocení na úrovni EAL1 se týká identifikace (čísla verze) produktu nebo systému IT, procedur instalace, generování a spuštění provozu, neformální specifikace funkcí, dokumentace správce a uživatele a provádí se nezávislé testování bezpečnostních funkcí.

6.8.2 EAL2, strukturálně testovaný produkt nebo systém IT

6.8.2.1 Cíle EAL2

- 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.

6.8.2.2 Záruky EAL2 (rozšíření proti EAL1)

- Požaduje se provedení analýzy návrhu produktu nebo systému IT na vysoké úrovni.
- Analýza se navíc podporuje důkazy, poskytnutými vývojářem, získanými testováním bezpečnostních funkcí, výběrovým nezávislým potvrzením výsledků testů vývojáře, analýzou síly bezpečnostních funkcí a důkazy vývojářova hledání obvyklých zranitelných míst (všeobecně známých zranitelných míst).
- Požaduje se důkaz bezpečných procedur dodávek a konfigurační seznam hodnoceného produktu nebo systému IT.
- Úroveň EAL2 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL1, poněvadž se po vývojáři požaduje, aby svůj produkt testoval a provedl analýzu zranitelných míst a provádí se nezávislé testování založené na detailnějších specifikacích hodnoceného produktu nebo systému IT.
- Hodnocení na úrovni EAL2 se proti úrovni EAL1 týká i konfiguračních položek správy konfigurace, procedur dodávek, popisu návrhu na vysoké úrovni, důkazů úplnosti testů bezpečnostní funkcionality, testování prováděného vývojářem i nezávislého testování třetí stranou, síly bezpečnostních funkcí a analýzy zranitelnosti provedené vývojářem.

6.8.3 EAL3, metodicky testovaný a kontrolovaný produkt nebo systém

6.8.3.1 Cíle EAL3

- 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.

6.8.3.2 Záruky EAL3 (rozšíření proti EAL2)

- Hodnotí se důkazy testování návrhu na vysoké úrovni. Požaduje se používání řídicích nástrojů ve vývojovém prostředí a správa konfigurace produktu nebo systému IT.
- Úroveň EAL3 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL2, poněvadž se požaduje úplnější testování pokrytí bezpečnostních funkcí a mechanismů a/nebo procedur, které poskytují jistou důvěru v to, že produkt nebo systém IT nebyl nějak narušen během vývoje.
- Hodnocení na úrovni EAL3 se proti úrovni EAL2 týká i autorizačních nástrojů správy konfigurace a pokrytí správy konfigurace, návrhu prosazení bezpečnosti na vysoké úrovni, identifikace bezpečnostních opatření při vývoji, analýzy pokrytí funkcionality testy a testů návrhu na vysoké úrovni a zkoumání návodů z hlediska možné zranitelnosti plynoucí z neúplnosti nebo nedokonalosti dokumentace.

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

6.8.4.1 Cíle EAL4

- 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.

6.8.4.2 Záruky EAL4 (rozšíření proti EAL3)

- Musí se provést analýza všech rozhraní a analýza podrobného (detailního) návrhu a implementace bezpečnostních funkcí. Požaduje se existence neformálního modelu bez-

pečnostní 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 hodnotit detailnější popis návrhu, 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.

6.8.5 EAL5, semiformálně navrhovaný a testovaný produkt nebo systém IT

6.8.5.1 Cíle EAL5

- 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.

6.8.5.2 Záruky EAL5 (rozšíření proti EAL4)

- Hodnotí se úplná implementace, používá se formální model bezpečnostní politiky a semiformální prezentace specifikace bezpečnostních funkcí a návrhu vysoké úrovně a semiformálním způsobem se demonstruje jejich vzájemná korespondence. Produkt nebo systém IT musí být navržen jako modulární produkt nebo systém.
- Testy se provádějí na úrovni detailního návrhu a ověřuje se analýza skrytých kanálů, provedená vývojářem.
- Správa konfigurace produktu IT musí být z hlediska komponent produktu nebo systému IT úplná a vyčerpávající.
- Úroveň EAL5 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL4, poněvadž se požaduje hodnocení semiformálních popisů návrhu, celé implementace bezpečnostních funkcí, požaduje se strukturovanější, a tudíž snadněji analyzovatelná architektura, analýza skrytých kanálů a požadují se vylepšené mechanismy a procedury,

které poskytují důvěru v to, že produkt nebo systém IT nebyl nějak narušen během vývoje nebo dodávky.

- Hodnocení na úrovni EAL5 se proti úrovni EAL4 týká i vývojových nástrojů správy konfigurace, používají se semiformální specifikace bezpečnostních funkcí a semiformální návrh na vyšší úrovni, hodnotí se implementace celé bezpečnostní funkcionality, na semiformální úrovni se hodnotí korespondence návrhu a implementace, používá se formální model bezpečnostní politiky, musí se používat implementační standardy a standardizovaný model celého životního cyklu, testování se provádí na úrovni detailního návrhu, požaduje se provedení analýzy skrytých kanálů a produkt nebo systém IT musí být odolný proti útokům střední síly.

6.8.6 EAL6, testovaný produkt nebo systém IT se semiformálně ověřovaným návrhem

6.8.6.1 Cíle EAL6

- 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.

6.8.6.2 Záruky EAL6 (rozšíření proti EAL5)

- Požaduje se strukturovaná prezentace implementace a detailního návrhu. Hodnocený předmět musí mít modulární, hierarchickou architekturu a vývojář musí provést systematickou analýzu skrytých kanálů.
- Vývojový proces musí mít strukturovaný charakter, správa konfigurace musí být úplná.
- Úroveň EAL6 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL5, poněvadž se požadují mnohem více vyčerpávající analýzy, strukturovaná reprezentace implementace, propracovanější architektura (hierarchické vrstvy), nezávislá mnohem více vyčerpávající analýza zranitelnosti, systematická identifikace skrytých kanálů a náročnější správa konfigurace a řídicí nástroje pro vývoj. Produkt nebo systém IT s úrovní EAL6 musí být odolný vůči útokům vedeným s velkou silou.

6.8.7 EAL7, testovaný produkt nebo systém IT s formálně ověřovaným návrhem

6.8.7.1 Cíle EAL7

- 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.

6.8.7.2 Záruky EAL7 (rozšíření proti EAL6)

- Požaduje se formální prezentace funkčních specifikací a návrhu vysoké úrovně, formálně musí být demonstrovatelná rovněž korespondence mezi návrhem vysoké úrovně a detailním návrhem, pokud je to možné. Návrh nesmí být složitý, musí se jednat o jednoduchý produkt nebo systém IT.
- Úroveň EAL7 představuje významně vyšší zaručitelnost bezpečnosti než úroveň EAL6, poněvadž se požaduje vyčerpávající analýza pomocí formálních prezentací, a dále formální prokázání korespondence návrhu vysoké úrovně a detailního návrhu a konečně rovněž vyčerpávající testování.

BIS - 2

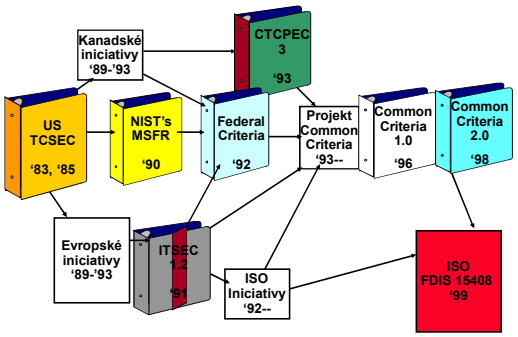
Act 2007, 2009pre

BIS
Bezpečnost informačních systémů

Petr Hanáček
Faculty of Information Technology
Technical University of Brno
Božetěchova 2
612 66 Brno
tel. 5 4114 1216
e-mail: hanacek@fit.vutbr.cz

Kritéria hodnocení bezpečnosti IS

Historie kritérií bezpečnosti IT



Pro koho jsou kritéria určena

- Uživatelé
- Vývojáři
- Hodnotitelé
- Jiní ...



Kritéria se nezabývají:

- ...administrativními opatřeními
- ...fyzickými aspekty bezpečnosti IT
- ...metodologií hodnocení
- ...dohodami o vzájemném uznávání
- ...kryptografickými *algoritmy*
- ...akreditací

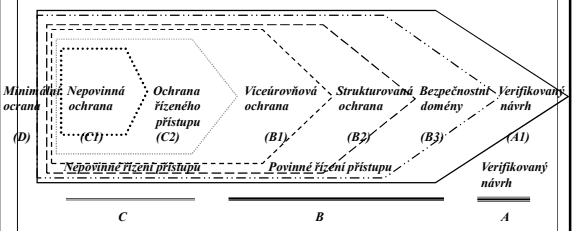
Orange Book

BIS - 2

Rainbow series

- Orange
  - Trusted Computer System Evaluation Criteria (TCSEC)
- Yellow
  - Guidance for Applying the Orange Book
- Red
  - Trusted Network Interpretation (TNE)
- Lavender (levandule)
  - Trusted Database Interpretation

Úrovně TCSEC



Požadavky úrovní

- C1: Discretionary Protection
  - Identifikace
  - Autentizace
  - Nepovinné řízení přístupu
- C2: Controlled Access Protection
  - Opětné použití a audit
- B1: Labeled security protection
  - Povinné řízení přístupu pro některé objekty
  - Neformální model bezpečnostní politiky
- B2: Structured Protections
  - Důvěryhodná cesta pro přihlášení
  - Princip nejmenších privilegií
  - Formální model bezpečnostní politiky
  - Analýza skrytých kanálů
  - Správa konfigurace
- B3: Security Domains
  - Mechanismus validace referencí (referenční monitor)
  - Omezení při vytváření kódu
  - Požadavky na dokumentaci a testování
- A1: Verified Protection
  - Formální metody pro analýzu a verifikaci
  - Důvěryhodná distribuce

Oblasti TCSEC

- Bezpečnostní politika
- Účtovatelnost
- Zaručitelnost
- Dokumentace
- Analýza skrytých kanálů
- Architektura systému
- Specifikace a verifikace návrhu

Bezpečnostní politika

	C1	C2	B1	B2	B3	A1
Nepovinné řízení přístupu (DAC)	+	+	nc	nc	+	nc
Opětné použití	0	+	nc	nc	nc	nc
Klasifikace dat (Labels)	0	0	+	+	nc	nc
Integrita klasifikace	0	0	+	nc	nc	nc
Export klasifikace	0	0	+	nc	nc	nc
Klasifikace neelektronických výstupů	0	0	+	nc	nc	nc
Povinné řízení přístupu (MAC)	0	0	+	+	nc	nc
Úroveň prověření uživatelů	0	0	0	+	nc	nc
Klasifikace zařízení	0	0	0	+	nc	nc

0 Žádné požadavky
\+ Dodatečné požadavky
nc Beze změny

Účtovatelnost

	C1	C2	B1	B2	B3	A1
Identifikace a autentizace	+	+	+	nc	nc	nc
Audit	0	+	+	+	+	nc
Důvěryhodná cesta	0	0	0	+	+	nc

0 Žádné požadavky
\+ Dodatečné požadavky
nc Beze změny

BIS - 2

Zaručitelnost

	C1	C2	B1	B2	B3	A1
Architektura systému	+	+	+	+	+	nc
Integrita systému	+	nc	nc	nc	nc	nc
Testování	+	+	+	+	+	+
Specifikace a verifikace návrhu	0	0	+	+	+	+
Analýza skrytých kanálů	0	0	0	+	+	+
Správa důvěryhodných zařízení	0	0	0	+	+	nc
Správa konfigurace	0	0	0	+	nc	+
Důvěryhodné zotavení	0	0	0	0	+	nc
Důvěryhodná distribuce	0	0	0	0	0	+

0 Žádné požadavky
\+ Dodatečné požadavky
nc Beze změny

©Petr Hanáček BIS Slide 13

Dokumentace

	C1	C2	B1	B2	B3	A1
Uživatelská dokumentace	+	nc	nc	nc	nc	nc
„Manuál důvěryhodných zařízení“	+	+	+	+	+	nc
Dokumentace k testům	+	nc	nc	+	nc	+
Dokumentace k návrhu	+	nc	+	+	+	+

0 Žádné požadavky
\+ Dodatečné požadavky
nc Beze změny

©Petr Hanáček BIS Slide 14

Analýza skrytých kanálů

B1 Bez požadavků
B2 Paměťové skryté kanály
B3 Všechny (paměťové i časové) skryté kanály
A1 Formální metody

©Petr Hanáček BIS Slide 15

Architektura systému

C1 DVB musí být schopna ochránit sama sebe
C2 DVB musí izolovat jednotlivé prostředky, o které se stará
B1 DVB musí zajistit dokonalou izolaci procesů
B2 DVB musí být strukturovaná do nezávislých, dobře definovaných modulů
B3 Návrh DVB musí využívat principy vrstevnatosti, abstrakce a skrývání dat
A1 Žádné dodatečné požadavky

©Petr Hanáček BIS Slide 16

Specifikace a verifikace návrhu

C2 Žádné požadavky
B1 Neformální nebo formální model bezpečnostní politiky
B2 Formální model bezpečnostní politiky u kterého je dokázaná konzistence
DTLS (descriptive top-level specification) modulu DVB
B3 DTLS musí být prokazatelně konzistentní s modelem
A1 FTLS (formal top-level specification) modulu DVB
FTLS musí být prokazatelně konzistentní s modelem
DTLS musí být prokazatelně konzistentní s modelem

©Petr Hanáček BIS Slide 17

Neoficiální pohled na úrovně

- **C1, C2**
  - Prosté vylepšení existujících systémů. Neohrožuje aplikace.
- **B1**
  - Závažnější rozšíření existujících systémů (především MAC). Některé aplikace vyžadují úpravy.
- **B2**
  - Zásadní změny oproti stávajícím systémům. Většina aplikací beze změn nebude fungovat.
- **B3**
  - Typicky systémy, které nezvládly A1
- **A1**
  - Systém musí být navržen a implementován od základu. Nutné využití entradičnic metod.

©Petr Hanáček BIS Slide 18

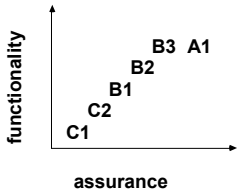
BIS - 2

Nedostatky TCSEC

- Směšuje v jednom dokumentu různé úrovně abstrakce
- Málo se zabývá integritou dat
  - Vojenský původ
- Kombinuje funkčnost a zaručitelnost do jedné lineární stupnice
- Nezná komunikaci a počítačovou síť
  - Publikace Trusted Network Interpretation (TNE) je nepoužitelná

Funkčnost a zaručitelnost

- TCSC nerozlišuje funkčnost a zaručitelnost
- Funkčnost (functionality)
  - Co je implementováno
- Zaručitelnost (assurance)
  - Jaká je míra důvěry, že je to správně
  - Lineární stupnice



Příklady ohodnocených produktù

- A1 - Secure Communications Processor (SCOMP), Release 2.1, Honeywell
- B2 - Multics MR11.0, Honeywell
- B1 - UNIX System V/MLS, Release 1.1.2 AT&T
- C2 - VAX/VMS Version 4.3 DEC
- C2 - SunOS, instalovaný pro C2 Sun Microsystems

UNIX ve třídě C2

Oproti standardnímu UNIXU je třeba změnit:

- opětné použití objektù
  - » disk, paměť, obrazovka
- NCSC prohlásilo, že řízení přístupu vyhovuje C2
- audit
  - » všechna přihlášení a odhlášení uživatelů
  - » všechny akce prováděné správcem
  - » maximální ochrana auditních dat
  - » oddělení auditních záznamù
- zašifrovaná hesla nesmí být přístupná (shadow)
- použitý procesor musí zajistit oddělení procesů
- 3 bezpečnostní příručky (uživatel, administrátor, technický popis)

NCSC - National Computer Security Center

Index rizika

- prostředek pro vyjádření požadované úrovně bezpečnosti
  - R_{min} - minimální úroveň prověření uživatele
  - R_{max} - maximální úroveň citlivosti dat
  - Index rizika = R_{max} - R_{min}

prověření uživatele	R_{min}
Neprověřený	0
Příst. k citlivým inf.	1
Prověřen pro důvěrné	2
Prověřen pro tajné	3
Prověřen pro přísně tajné	4

citlivost dat	R_{max}
Neklasifikovaná	0
Neklasifikovaná, citlivá	1
Důvěrná	2
Tajná	3
Přísně tajná	4

Index rizika (pokr.)

- minimální třída bezpečnosti systému pro daný index rizika:

Index rizika	otevřené prostředí	uzavřené prostředí
0	C2	C2
1	B1	B1
2	B2	B2
3	B3	B2
4	A1	B3
5	-	A1

BIS - 2

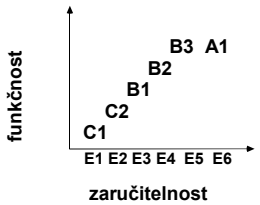
ITSEC

ITSEC

- ITSEC: IT Security Evaluation Criteria
- Vytvořena z národních kritérií UK, Německa, Francie a Holandska
- Výstupy
  - ITSEC: 1991
  - ITSEM: 1993 (IT Security Evaluation Manual)
  - UK IT Security Evaluation & Certification scheme: 1994

ITSEC - Metodologie

- Založené na systematickém a dokumentovaném přístupu k hodnocení
- Rozlišují produkty a systémy
- Dva rozměry
  - Funkčnost
  - Zaručitelnost



ITSEC – Třídy funkčnosti

- Přístup 1:
  - F-C1, F-C2, F-B1, F-B2, F-B3
  - Třídy odpovídající stejnojmenným úrovním TCSEC
- Přístup 2:
  - F-IN
    - » Systémy se zvýšenými nároky na integritu
  - F-AV
    - » Systémy se zvýšenými nároky na dostupnost
  - F-DI
    - » Systémy se zvýšenými nároky na integritu přenosu dat
  - F-DC
    - » Systémy se zvýšenými nároky na důvěrnost přenosu dat
  - …

ITSEC - Zaručitelnost

- E1: Security target defined, tested
  - Must have informal architecture description
- E2: Informal description of design
  - Configuration control, distribution control
- E3: Correspondence between code and security target
- E4: Formal model of security policy
  - Structured approach to design
  - Design level vulnerability analysis
- E5: Correspondence between design and code
  - Source code vulnerability analysis
- E6: Formal methods for architecture
  - Formal mapping of design to security policy
  - Mapping of executable to source code

ITSEC - síla mechanismů

- Síla mechanismů je podle ITSEC (odstavce 3.6-3.8):
  - základní
  - střední
  - vysoká
- Význam:
  - a) <u>základní</u>
    mechanismus chrání proti náhodným poruchám, avšak může být narušen kvalifikovanými útočníky.
  - b) <u>střední</u>
    mechanismus chrání proti útočníkům s omezenými příležitostmi a prostředky.
  - c) <u>vysoká</u>
    mechanismus může být narušen pouze útočníky, disponujícími vysokou úrovní znalostí, příležitostmi a prostředky rovněž na vysoké úrovni a úspěšný útok se vymyká běžné praxi.
- Vágní definice - v praxi nepoužitelná

BIS - 2

ITSEM - síla mechanismů

- Síla mechanismů bere v úvahu
  - znalosti
  - prostředky
  - příležitost útočníka
- 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.
- Prostředky
  - objem prostředků, které musí útočník vynaložit k úspěšnému útoku na systém. Jsou dvojí - čas a vybavení.
    - » Čas - doba, kterou útočník potřebuje na provedení útoku
      - v minutách - do deseti minut
      - ve dnech - do jednoho měsíce
      - v měsících - útok trvá více než měsíc
    - » Vybavení - počítače, elektronická zařízení, technické prostředky a programy.
      - bez vybavení - není potřebné žádné speciální vybavení
      - běžné vybavení - vybavení, které je běžně dostupné v provozním prostředí HP
      - speciální vybavení - speciální jednoúčelové vybavení

- Příležitost
  - zahrnuje faktory, které obecně není schopen útočník ovlivnit
    - » požadavek na asistenci jiné osoby (komplot)
    - » pravděpodobnost výskytu jisté speciální kombinace okolností (šance)
    - » pravděpodobnost a následky odhalení útočníka (detekce)
  - formy komplotu:
    - » samostatný, pokud žádný komplot není potřeba
    - » s uživatelem, pokud je pro úspěch útoku třeba komplot mezi útočníkem a (nedůvěryhodným) uživatelem HP
    - » se správcem, pokud je třeba komplot s vysoce důvěryhodným u ivatelem HP
  - Tato definice komplotu předpokládá, že útočník není autorizovaným uživatelem HP

Tabulka pro čas a komplot

	samostatný	s uživatelem	se správcem
v minutách	0	12	24
ve dnech	5	12	24
v měsících	16	16	24

Tabulka pro znalosti a vybavení

	bez vybavení	běžné vybavení	speciální vybavení
začátečník	1	-	-
zkušený	4	4	-
expert	6	8	12

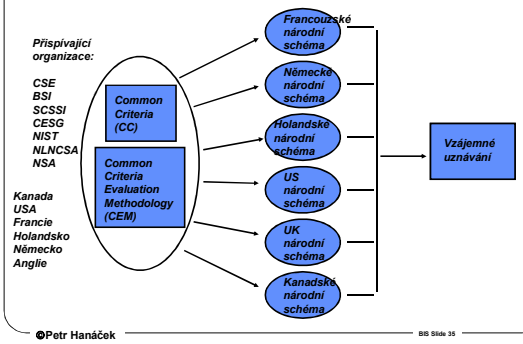
Je třeba sečíst hodnoty, získané z tabulek:

v=1	síla není ani základní.
1<v<12	síla je základní.
12<v<24	síla je střední.
24<v	síla je vysoká.

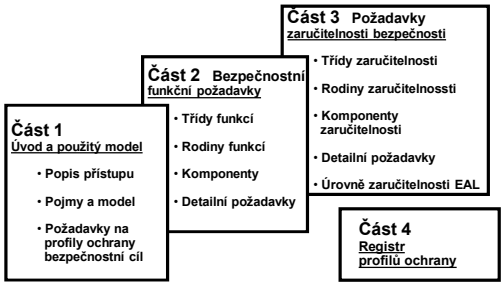
Hodnocení bezpečnosti IT podle normy ISO/IEC 15408 (Common Criteria)

Petr Hanáček
Fakulta informačních technologií
VUT Brno
hanacek@fit.vutbr.cz

Kontext kritérií



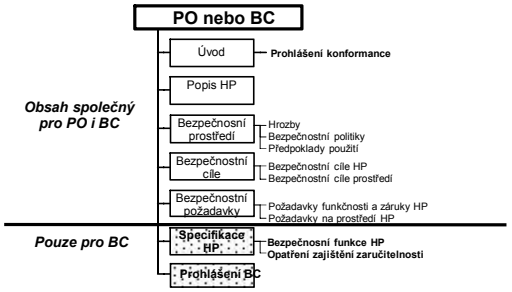
Struktura ISO 15408 / CC



BIS - 2

Profil ochrany a bezpečnostní cíl

- PO - Pro kategorii produktů
- BC - Pro konkrétní typ produktu



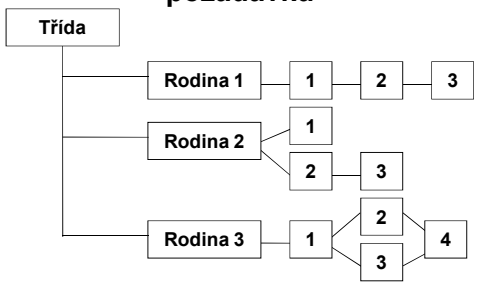
Část 2 - Třídy funkčních požadavků

- Třída FAU: Bezpečnostní audit (35 komponent)
- Třída FCO: Komunikace (4)
- Třída FCS: Kryptografická podpora (40)
- Třída FDP: Ochrana uživatelských dat (46)
- Třída FIA: Identifikace a autentizace (27)
- Třída FMT: Správa bezpečnosti
- Třída FPR: Soukromí (8)
- Třída FPT: Ochrana bezpečnostní funkcionality (43)
- Třída FRU: Využití zdrojů (8)
- Třída FTA: Přihlášení do HP (11)
- Třída FTP: Důvěryhodné cesty/kanály (2)

Hierarchie pojmů

- Třída (např. FDP - Ochrana uživatelských dat): seskupení rodin, které jsou stejně zaměřeny
- Rodina (např. FDP_ACC - Politika řízení přístupu): seskupení komponent, které mají stejný bezpečnostní cíl ale různou sílu nebo přísnost
- Komponenta (např. FDP_ACC.1 - Řízení přístupu k podmnožinám): nejmenší volitelná sada prvků, která může být použita v BC nebo PO

Část 2 - Hierarchie funkčních požadavků



Zaručitelnost - Assurance

- Slovníková definice: (Oxford)
  - a positive declaration that a thing is true
  - a promise or guarantee
  - certainty
- Definice podle CC:
  - *grounds for confidence that an IT product or system meets its security objectives*
- Je ochranou proti:
  - špatnému návrhu
  - implementačním chybám
  - neefektivním opatřením nebo mechanismům

Část 3 - Evaluation Assurance Levels (EALs)

EAL	Jméno	*TCSEC
EAL1	funkčně testovaný	
EAL2	strukturálně testovaný	C1
EAL3	metodicky testovaný a kontrolovaný	C2
EAL4	metodicky navrhovaný, testovaný a přezkoumávaný	B1
EAL5	semiformálně navrhovaný a testovaný	B2
EAL6	testovaný se semiformálně ověřovaným návrhem	B3
EAL7	testovaný s formálně ověřovaným návrhem	A1

*TCSEC = "Trusted Computer Security Evaluation Criteria" --"Orange Book"

BIS - 2

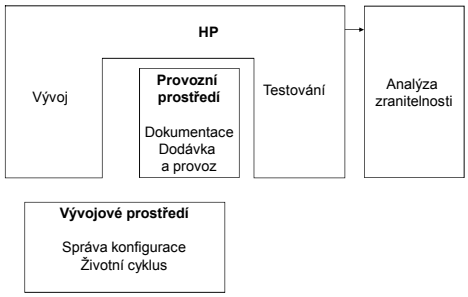
EAL

- EAL1 - (nová)
  - Nejnižší úroveň pro hodnocení
- EAL2 - (odpovídá C1 - E1)
  - Nejlepší, čeho lze dosáhnout bez dodatečné práce vývojáře
- EAL3 - (odpovídá C2 - E2)
  - Dovoluje uvědomělému vývojáři získat bezpečný návrh bez závažných změn vývojových postupů
- EAL4 - (odpovídá B1 - E3)
  - Nejlepší, čeho lze dosáhnout bez závažných změn vývojových postupů
- EAL5 - (odpovídá B2 - E4)
  - Nejlepší, čeho lze dosáhnout pomocí plánovaného a kvalitního vývoje bez extrémně vysokých nákladů
- EAL6 - (odpovídá B3 - E5)
  - "high tech" úroveň pro typicky vojenské použití
- EAL7 - (A1 - E6)
  - Nejvyšší dosažitelná bezpečnost, hranice současné technologie

Třídy požadavků zaručitelnosti

- ACM: Správa konfigurace
  - Automatizace správy konfigurace, Akceptační procedury
- ADO: Dodávka a provoz
  - Detekce modifikace, Procedury pro instalaci, generování a start
- AGD: Dokumentace
  - Dokumentace pro uživatele a správce
- ALC: Podpora životního cyklu
  - Definovaný model životního cyklu, Definované vývojové nástroje
- AVA: Analýza zranitelnosti
  - Analýza síly bezpečnostních funkcí, Nezávislá analýza zranitelnosti
- ADV: Vývoj
  - Model Bezpečnostní politiky, Funkční specifikace, Model architektury, Detailní model, Důkaz korespondence
- ATE: Testování
  - Testování podle Funkční specifikace, Modelu architektury, Analýza pokrytí testů

Uplatnění tříd záruky



Úroveň záruky EAL 4

- Podle definice "metodicky navrhovaný, testovaný a přezkoumávaný produkt nebo systém IT"
- Umožňuje svědomitému vývojáři dosáhnout maximálně možnou zaručitelnost bezpečnosti, založenou na dobrých komerčních vývojových praktikách, které nepožadují mimořádně velké odborné znalosti, dovednosti a jiné zdroje
- Používá některé formální postupy
- Nejvyšší úroveň pro běžně vyráběné produkty

Neformální, poloformální, formální

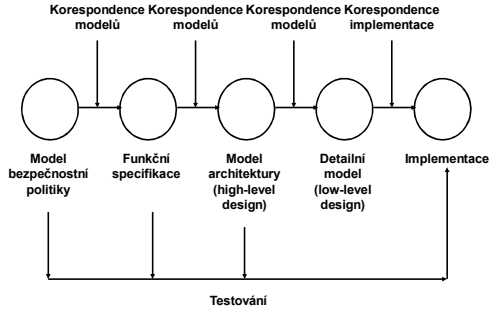
- Neformální model/specifikace
  - zapsána v přirozeném jazyce
  - nepodléhá žádným speciálním omezením
- Poloformální model/specifikace
  - vyžaduje užití některé omezující notace (nebo notací) spolu s množinou konvencí
  - může mít buď grafickou podobu, nebo může být založen na omezeném užití přirozeného jazyka
  - např. grafy toku dat, diagramy vzájemných vztahů mezi entitami a relacemi, grafy datových struktur, grafy struktury procesu nebo programu, notace SDL doporučená CCITT.
- Formální model/specifikace
  - zapsána ve formální notaci, která využívá dobře definovaných matematických pojmů
  - např. metoda VDM, Z notace, RAISE Specification Language, Gypsy Specification Language, ISO Protocol Specification Language

Jednotlivé modely při vývoji

- Model bezpečnostní politiky
  - popisuje komponenty bezpečnostní politiky, které jsou zabezpečeny bezpečnostními funkcemi
- Funkční specifikace
  - popis bezpečnostních funkcí a externích rozhraní
- Model architektury (high-level design)
  - popis posloupnosti akcí, které jsou provedeny v každém subsystému na základě stimulu na jeho rozhraní
- Detailní model (low-level design)
  - popis realizace posloupnosti akcí, které jsou provedeny v každém subsystému na základě stimulu na jeho rozhraní
  - musí obsahovat všechny identifikovatelné komponenty (např. funkce, procedury atd.)
- Implementace

BIS - 2

Vývoj



CEM - Common Evaluation Methodology

- Doplněk k CC
- Popisuje aktivity hodnotitele
- Důležitá pro vzájemné uznávání
- Část 1: Úvod a obecný model
  - Terminologie a principy hodnocení
- Část 2: Metodologie hodnocení
  - PO a BC
  - EAL 1-4
  - EAL 5-7
- Část 3: Rozšíření metodologie

Management bezpečnosti

Celková bezpečnostní politika (CBP)

- Globální popis cílů organizace, jejího IS a zabezpečení
- Cíl
  - ochrana majetku, pověsti a činnosti instituce
- Dokument
  - nadčasový, nezávislý na použité technologii, (horizont 5-10 let)
  - přijatý vedením organizace jako vnitroinstitucionální norma
  - závazný dokument, veřejný dokument
- Stanovuje
  - citlivé informace, ostatní citlivá aktiva a jejich klasifikaci
  - jednoznačné (hierarchické) zodpovědnosti & práva & pravomoci
  - minimální sílu použitých bezpečnostních mechanismů
- Stručný a srozumitelný, úplný dokument
  - otázky a konflikty lze vyřešit odkazem na paragrafy CBP

Příklad struktury CBP

- Popis organizace, jejího poslání a koncepcí IT organizace
- Rámcový plán a harmonogram vybudování celkové bezpečnostní politiky
- Cíle CBP
- Specifikace potřebné struktury zodpovědnosti a pravomocí
- Identifikace (kritických) aktiv, zvláště pak citlivých dat
- Identifikace obecných hrozeb
- Výsledky orientační analýzy rizik
- Popis stávajícího stavu zabezpečení
- Doporučení, jak dosáhnout bezpečnostních cílů
- Cíle a strategie havarijních plánů
- Omezení respektovaná bezpečnostní politikou
  - návaznosti na relevantní zákony, vyhlášky a předpisy
- Časové plány implementace a pravidelných akcí, revizí/oprav
- Návrh a koncepce programu školení a osvěty

Systémová bezpečnostní politika (SBP)

- Systémová bezpečnostní politika
  - Definuje způsob implementace celkové bezpečnostní politiky IT v konkrétním prostředí
  - Stanovuje soubor principů a pravidel pro ochranu IS
  - Zabývá se volbou konkrétních technických, procedurálních, logických a administrativních bezpečnostních opatření
  - Částečně i volbou fyzických a personálních bezpečnostních opatření, pokud tyto mohou ovlivnit bezpečnost IS
  - Implicitně se zabývá bezpečností elektronické (počítačové) části IS
  - Pokud je IS příliš rozsáhlý a různorodý, je vhodné vypracovat samostatně systémovou bezpečnostní politiku pro různé oblasti nebo subsystémy

BIS - 2

Tvorba bezpečnostní politiky

- BP nikdy nevzniká jednorázovou akcí
- životní cyklus tvorby BP lze zjednodušeně vyjádřit následujícími (opakovaně) prováděnými kroky
  - 1. posouzení vstupních vlivů
  - 2. analýza rizik
  - 3. vypracování BP
  - 4. implementace BP
  - 5. nasazení BP, kontrola její účinnosti a vyslovování závěrů

Normy a standardy

- TR 13335 - Guidelines for the Management of IT Security
  - ČSN ISO/IEC TR 13335 Informační technologie – Směrnice pro řízení bezpečnosti IT 1-3
- BS7799 - Code of Practice for Information Security Management
  - ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti
- ISO 27001
  - nová mezinárodní norma pro Systém správy informační bezpečnosti (Information Security Management System, ISMS)

TR 13335

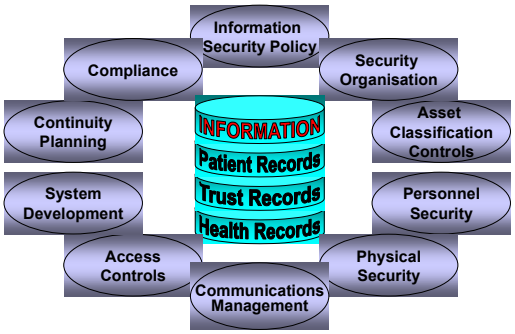
- Part 1: Concepts and Models for IT Security
- Part 2: Managing and Planning IT Security
- Part 3: Techniques for the Management of IT Security
- Part 4: Selection of Safeguards
- Part 5: Safeguards for External Connections

TR 13335 - Proces bezpečnosti IT

BS7799 - Code of Practice for Information Security Management

- Britský standard, který je používán i v jiných evropských zemích
- Určen jako referenční dokument pro osoby zodpovědné za implemementaci a udržování informační bezpečnosti v organizaci
- Certifikační schéma, zvané c:cure, podobné ISO 9000
- Přijato jako norma ISO/IEC 17799:2000
  - ČSN ISO/IEC 17799 Informační technologie – Soubor postupů pro řízení informační bezpečnosti
- 1. ISO 17799 definuje 10 řídicích principů
- 2. BS 7799-2:1999 obsahuje:
  - 36 cílů
  - 127 opatření

Principy BS 7799



BIS - 2

Bezpečnostní politika

- Určuje směr zabezpečení a zajišťuje manažerskou podporu
  - Existence BP v organizaci
  - Správa a aktualizace BP

Organizace bezpečnosti

- Správa bezpečnosti v organizaci
- Bezpečnostní infrastruktura
  - Definice rolí, povinností a odpovědností
  - Koordinace
  - Allocation of information security responsibilities
- Outsourcing

Klasifikace a správa aktiv

- Klasifikace hodnoty a kritičnosti aktiv
- "Kritická aktiva"

Personální bezpečnost

- Je namířena přímo na osoby (nikoli prostřednictvím IS)
- Je převážně preventivní
- Je založena na
  - » důvěryhodnosti pracovníka
  - » spolehlivosti pracovníka

Fyzická bezpečnost

- Fyzická bezp. opatření fyzickým způsobem omezují přístup ke komponentám informačního systému
- Zabraňují hrozbám pro fyzické komponenty systému

Komunikace a provoz

- Především administrativní bezpečnostní opatření
- Bezpečnostní procedury, prováděné lidmi

Řízení přístupu

- Povolit pouze oprávněný přístup k informacím, službám a dalším prostředkům
  - Ochrana před ztrátou, prozrazením, modifikací nebo podvržení informací

Vývoj a údržba systému

- Zajištění bezpečnosti životního cyklu systému

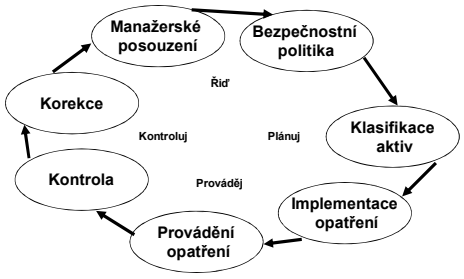
Zajištění kontinuity

- Cíl: zabránit přerušení obchodních aktivit a ochránit kritické procesy před výpadky
- Havarijní plány

Shoda

- Jde především o shodu se zákony a jinými normami

Implementace BS 7799



BIS - 2

ISO 27001

- ISO 27001 je nová mezinárodní norma pro Systém správy informační bezpečnosti (Information Security Management System, ISMS)
- Postupně nahradí BS7799-2
  - Specifikuje požadavky na zavedení ISMS
- ISO 27001 je první normou v nové sérii mezinárodních norem pro správu bezpečnosti
- Je harmonizována s:
  - ISO9001:2000 (Quality Management System)
  - ISO14001:1996 (Environmental Management System)

ISO 27001 - Oblasti

- Security policy
  - Bezpečnostní politika
- Organisation of information security
  - Organizace informační bezpečnosti
- Asset management
  - Správa aktiv
- Human resources security
  - Personální bezpečnost
- Physical and environmental security
  - Fyzická bezpečnost
- Communications and operations management
  - Bezpečnost komunikací a provozu

ISO 27001 - Oblasti

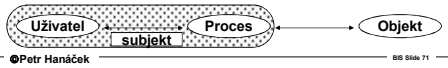
- Access control
  - Řízení přístupu
- Information systems acquisition, development and maintenance
  - Pořizování, vývoj a údržba
- Information security incident management
  - Správa bezpečnostních incidentů
- Business continuity management
  - Správa kontinuity
- Compliance
  - Shoda

Modely bezpečnosti

Modely bezpečnosti

Formální vyjádření části bezpečnostní politiky

- podle řízení přístupu
  - povinné řízení přístupu
  - nepovinné řízení přístupu
- podle klasifikace informace
  - jednoúrovňové X víceúrovňové
- podle cílů, které zajišťují
  - modely důvěrnosti
  - modely integrity
  - modely dostupnosti
- entity
  - uživatel, proces, objekt, subjekt



Monitor

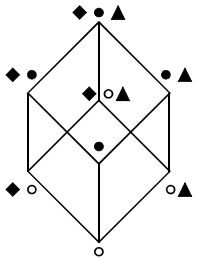
- Definován v Orange Book
- Prostředek pro lokalizaci bezpečnostních funkcí do jednoho místa
- Požadavky
  - nelze jej obejít
  - je odolný proti útoku (schopen zajistit vlastní integritu)
  - malý, aby mohl být podroben analýze správnosti

BIS - 2

Víceúrovňové modely

- **Stupeň utajení**
  neklasifikovaná < důvěrná < tajná < přísně tajná
- **Kategorie**
  osobní, obchodní, ...
- **Bezpečnostní atributy**
  <stupeň utajení, kategorie>
- **Relace <=**
  - O<=S jen tehdy, pokud
    stupeň-utajení$_O$ <= stupeň-utajení$_S$ a
    kategorie$_O$ ⊆ kategorie$_S$

Svazový model pro více úrovní

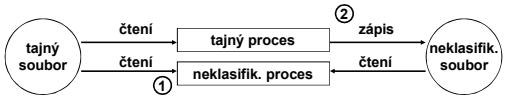


○ neklasifikované ◆ osobní
● tajné ▲ obchodní

- **transitivita**
  - if a<=b and b<=c then a<=c
- **antisymetrie**
  - if a<=b and b<=a then a=b
- **nejvyšší prvek**
  - <tajné, {osobní, obchodní}>
- **nejnižší prvek**
  - <neklasifikované, {}>
- **některé prvky jsou neporovnatelné**
  - <tajné, osobní>
  - <tajné, obchodní>

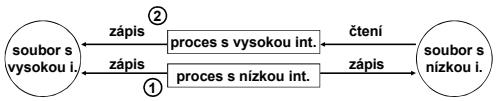
Bell-LaPadulův model důvěrnosti

- **Ohodnocení subjektu a objektu**
  - stupeň důvěry v subjekt *C(s)*
  - úroveň důvěrnosti objektu *C(o)*
- **Jednoduchá ochrana (1)**
  - subjekt *s* může číst objekt *o*, pokud
    C(s) >= C(o)
- **Omezující vlastnost (*-vlastnost) (2)**
  - pokud subjekt *s* může číst objekt *o*, pak může modifikovat objekt *p*, pokud *C(p) >= C(o)*

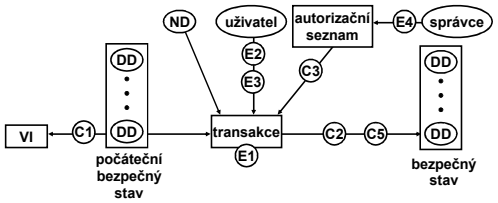


Bibův model integrity

- **Je duálním modelem k Bell-LaPadulovu modelu**
  - stupeň důvěry v subjekt *I(s)*
  - úroveň integrity objektu *I(o)*
- **Jednoduchá ochrana (1)**
  - subjekt *s* může modifikovat objekt *o*, pokud
    I(s) >= I(o)
- **Omezující vlastnost (*-vlastnost) (2)**
  - pokud subjekt *s* může číst objekt *o*, pak může modifikovat objekt *p*, pokud *I(o) >= I(p)*



Clark-Wilsonův model integrity



- DD - důvěryhodná data
- ND - nedůvěryhodná data
- VI - verifikace integrity
- E1 - DD je měněno autorizovanou transakcí
- E2 - uživatel je autentizován
- E3 - uživatel je autorizován
- E4 - autorizaci mění pouze správce
- C1 - VI zkontroluje, že DD jsou bezpečná
- C2 - TP zachovává bezpečnost dat
- C3 - oddělení pravomocí
- C4 - transakce změní ND na DD

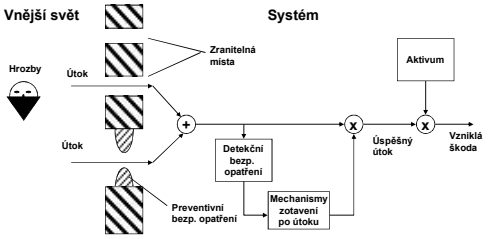
Modely dostupnosti

- **Systém kvót**
  - každý uživatel má omezeno množství prostředků, které mu lze přidělit
    - » prostor na disku, prostor v paměti, čas procesoru, délka relace, počet tiskových stran....
- **Amorosův model**
  - každý uživatel má prioritu *p* a prostředek kritičnost *c*
  - funkce *prevent(p,c)* říká, zda se má prostředek uživateli poskytnout
- **Yu-Gligorův model**
  - spravedlnost - uživatel nebude blokován navždy, pokud je možnost, aby pokračoval
  - simultánnost - uživatel někdy dostane všechny možnosti, jak pokračovat
  - dohoda uživatelů - současné požadavky uživatelů na službu jsou uspořádány podle analýzy všech ostatních požadavků

BIS - 2

Analýza rizik

Model incidentu



Proces analýzy rizik

- Identifikace aktiv
- Stanovení zranitelných míst a hrozeb
- Stanovení rizik
- Výpočet očekávané roční ztráty (ALE, Annual Loss Expectations)
- Volba bezpečnostních opatření
- *Určení ročních úspor*

Výpočet ALE

- Riziko
  - škodlivý efekt uskutečnění hrozby
  - škodlivý efekt využití zranitelného místa
- Riziko závisí na :
  - P - pravděpodobnost výskytu bezpečnostního incidentu (např. v jednotkách výskytů za rok)
  - C - průměrná škoda vzniklá tímto incidentem
- Riziko se vypočte jako

$$R = P \,.\, C$$

- Příklad: Organizace má problémy s neoprávněným přístupem k počítačové síti. Panuje obava, že útočník může získat přístup k důvěrným informacím nebo neoprávněně používat výpočetní prostředky organizace.
- Rizika:
  - Neautorizovaný přístup k datům
    - » Pravděpodobnost výskytu události 1/tři roky
    - » Vzniklá škoda 600 000
    - » Celkem 200 000
  - Neautorizovaný přístup k výpočetním prostředkům
    - » Pravděpodobnost výskytu události 5/rok
    - » Vzniklá škoda 6 000
    - » Celkem 30 000
  - ALE 230 000
- Efektivnost systému pro řízení přístupu: 90% -207 000
  - Cena systému pro řízení přístupu:
    - » Hardware (50 000, amortizace 5 let) 10 000
    - » Software (30 000, amortizace 5 let) 6 000
    - » Roční náklady na údržbu 50 000
    - » Celková cena 66 000
  - ALE (po aplikaci systému pro řízení přístupu)
    - » 230 000 - 207 000 + 66 000 = 89 000
    - » Roční úspory (230 000 - 89 000) = 141 000

Generace analýzy rizik

- 1972… Metody „Checklist“
  - Výběr z několika řešení na základě dotazníku
- 1981… Mechanistické inženýrské metody
  - Dělení složitých řešení na podúlohy a části
- 1988… Logické transformační
  - Abstrakce problému a řešení
- 1994… Organizačně řízené
  - Hledá se řešení i v netechnických oblastech

BIS - 2

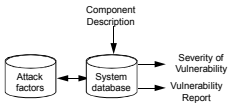
1. Generace

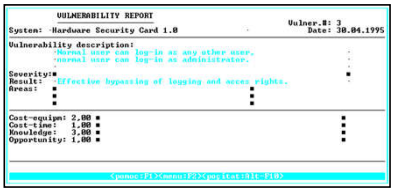
- Vlastnosti metod první generace
- Předpoklady:
  - oblast možných řešení je silně omezena
  - každé z řešení je značně univerzální
  - vliv bezpečnostních opatření je vyjádřen jako snížení pravděpodobnosti výskytu hrozby nebo snížení vlivu hrozby

VULAN

- Oblast zranitelnosti
- Míra příležitosti útočníka
- Míra znalostí útočníka
- Čas potřebný pro útok
- Vybavení potřebné pro útok

Výsledkem je zjištěná míra zranitelnosti komponenty.



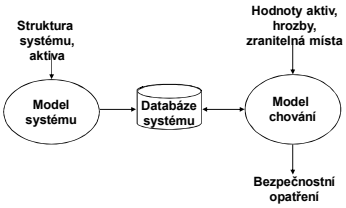


2. Generace

- Druhá generace - Mechanistické inženýrské metody
- Vlastnosti:
  - zobrazují problém do velkého množství částečných řešení
- Vývojové prostředky:
  - návrh shora dolů
- Bezpečnostní prostředky:
  - Zjišťují odděleně:
    - » Aktiva
    - » Hrozby
    - » Zranitelná místa

Model analýzy rizik

- Volbu různých alternativ bezpečnostních opatření může výrazně usnadnit automatizovaný přístup založený na vhodném modelu
- Struktura
  - Model systému
  - Model chování

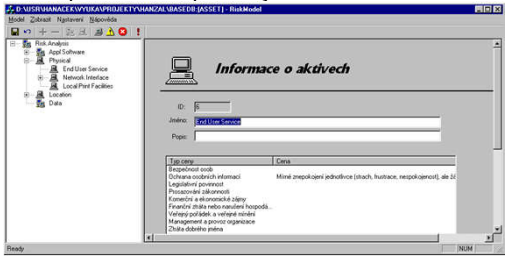


Struktura aktiv

- Data Asset
  - End User Service
    - Non-Network Hosts, Network Hosts
      - Location
    - Non-Network Workstations, Network Workstations
      - ....
    - Local Storage Facility, Network Storage Device
    - Local Print Facility, Network Print Server
    - Network Distribution Component
    - Network Gateway
    - Network Management/Operation Host
    - Network Interface
    - Network Service
    - Communications Protocols.
  - Application Software
    - » Hosts and Workstations
      - Location
  - Media
    - » Location

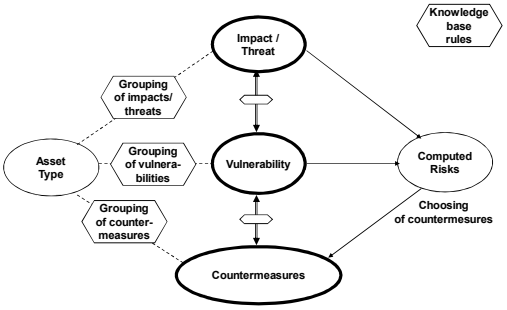
Vytváření a ohodnocení aktiv

- Operace
  - Vytváření struktury aktiv a seskupování
  - Ohodnocení zranitelných míst a hrozeb
  - Export modelu do expertního systému



BIS - 2

Příklad modelu chování



Dotazník pro zjištění hrozeb

Threat : Masquerading of User Identity by Insiders

Threat Questionaire

1 How many attempts have been made by insiders, during the last three years, to gain unauthorised access to information on the system/network by using another user's account?

Possible Answers

a	None	0
b	Once or twice	10
c	On average once a year	20
d	On average more than once a year	30
e	Unknown	10

2 What is the trend of attempts to gain unauthorised access to the system / network in this manner?

Possible Answers

a	Increasing	10
b	Remaining constant	0
c	Decreasing	-10

3 Does the system / network hold information which would motivate insiders to gain unauth access to the information e.g. personnel files

Possible Answers

a	Yes	5
b	No	0

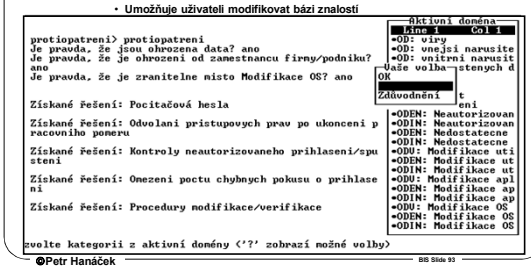
4 Have there been any discovered attempts to subvert insiders by outsiders?

Possible Answers

a	Yes	10
b	No	0

Komunikace s modelem

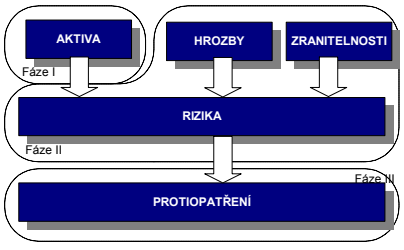
- **Dotazování**
  - Uživatel klade systému dotazy a ten se snaží na základě aktuální báze znalostí odvodit správnou odpověď
- **Prohlížení znalostí**
  - Umožňuje uživateli zobrazit bázi aktuálních znalostí
- **Editace stávající báze znalostí**
  - Umožňuje uživateli modifikovat bázi znalostí



CRAMM

- **Vytvořen původně v roce 1985, stále aktualizován**
- **CRAMM Risk Analysis Methodology je balík, obsahující:**
  - **Správu procesu analýzy rizik**
  - **Sovisející dokumentaci (např. reporty, výsledky a závěry)**
  - **Školení**
  - **Podpůrné softwarové nástroje**

Analýza a řízení rizik pomocí CRAMM



3. Generace

- **Třetí generace - Logicko-transformační metody**
- **Vychází z toho, že model pro analýzu rizik musí znát nejenom strukturu systému, ale i jeho funkčnost**
- **Např. SSADM-CRAMM**

BIS - 2

Námitky proti analýze rizik

- **Nepřesná**
  - Odhady bývají nepřesné a výsledku různých metodologií se často liší
- **Vyvolává falešný dojem přesnosti**
  - Špatná interpretace výsledků není chybou metodologie ale chybou uživatele
- **Neměnnost**
  - Uživatelé často provedou analýzu rizik jednou a nikdy ji neopakují. Analýza rizik by měla být opakována při každé významné změně vnějších okolností.
- **Nemá vědecký základ**
  - Většina metodologií má vědecký základ.

©Petr Hanáček BIS Slide 97

KONEC

©Petr Hanáček BIS Slide 98