Kritéria hodnocení informační bezpečnosti, dodatek

PV 017 ◇ Bezpečnost IT

Jan Staudek
http://www.fi.muni.cz/usr/staudek/vyuka/

Verze : podzim 2019

Doplněk přednášky pro samostudium

- Následující podklady jsou doplňkem přednášky určený pro rozšířující samostudium

EALs, Evaluation Assurance Levels, přehled

- *Evaluation assurance level 1 (EAL1) - functionally tested*
  - ✓ *EAL1 provides an evaluation of the TOE as made available to the customer,*
  - ✓ *including independent testing against a specification, and an examination of the guidance documentation provided.*
  - ✓ *It is intended that an EAL1 evaluation could be successfully conducted without assistance from the developer of the TOE, and for minimal outlay.*
  - ✓ *An evaluation at this level should provide evidence that the TOE functions in a manner consistent with its documentation.*
- požaduje se správný (bezchybný) provoz TOE
- žádné hrozby nejsou považované pro TOE za závažné

Charakteristiky EAL1, funkčně testovaný TOE

- požaduje se získání nezávisle vyslovené záruky podporující tvrzení, že byla vynaložena patřičná starost o ochranu např. osobních dat
- Důvěra EAL1 se dosahuje
  - ✓ nezávislým testováním shody hodnoceného PP, ST nebo TOE s jeho neformální funkční specifikací a
  - ✓ zkoumáním předložených příruček pro uživatele, zda jim funkčnost TOE odpovídá
- hodnocení
  - ✓ je proveditelné bez spoluúčasti a bez pomoci vývojáře
  - ✓ vyžaduje vynaložení minimálních nákladů
  - ✓ má poskytnout důkazy o tom, že TOE funguje v souladu s dokumentací a poskytuje dobrou ochranu proti identifikovaným hrozbám
- cílová EAL při zabezpečování systémů obsahujících např. pouze osobní údaje, evidenci DKP, . . .

EALs, Evaluation Assurance Levels, přehled

- *Evaluation assurance level 2 (EAL2) - structurally tested*
  - ✓ *EAL2 is applicable in those circumstances where developers or users require a low to moderate level of independently assured security in the absence of ready availability of the complete development record.*
  - ✓ *Such a situation may arise when securing legacy systems, or where access to the developer may be limited.*

Charakteristiky EAL2, strukturálně testovaný TOE

- vyžaduje spolupráci vývojáře, vývojář musí dodat
  - ✓ funkční specifikace
  - ✓ určité informace o návrhu bezpečnostních funkcí (na úrovni globálního návrhu, high-level design) a
  - ✓ výsledky testování provedené vývojářen
- vývoj si nevyžaduje více úsilí nežli je potřebné pro dodržování dobré komerční praxe
  - ✓ vhodná EAL pro případy, kdy je vývojář dostupný omezeně
- vývoj nezpůsobuje zvýšení nákladů
- EAL2 vyjadřuje nízkou až střední nezávisle ověřenou záruku za dosaženou bezpečnost v případě, že není dostupná kompletní informace z fáze vývoje

Charakteristiky EAL2, strukturálně testovaný TOE

- Úroveň záruky za dosažení bezpečnosti EAL2 vyžaduje
  - ✓ splnění podmínek stanovených pro EAL1
  - ✓ provedení analýzy vyžádané dokumentace
  - ✓ ověření výsledků některých testů
  - ✓ provedení analýzy síly funkcí a
  - ✓ provedení analýzy ošetření obecně známých zranitelností
- Pro TOE musí být
  - sestavený seznam konfigurace
  - vypracovány procedury pro bezpečnou instalaci, generování a spuštění
- cílová EAL při zabezpečování systémů typu podnikové účetnictví

EALs, Evaluation Assurance Levels, přehled

- *Evaluation assurance level 3 (EAL3) -*
  methodically tested and checked
  - ✓ *EAL3 is applicable in those circumstances where developers or users require a moderate level of independently assured security, and require a thorough investigation of the TOE and its development without substantial re-engineering.*
  - ✓ EAL3 represents a meaningful increase in assurance from EAL2 by requiring more complete testing coverage of the security functionality, mechanisms and/or procedures that provide some confidence that the TOE will not be tampered with during development

EAL3, metodicky testovaný a kontrolovaný TOE

- maximálně vysoká úroveň záruky dosažení bezpečnosti vyslovitelná na základě zjištění, že se při návrhu průkazně použilo bezpečnostní konstruování, a to aniž by vývojář musel podstatně měnit své dobré vývojové praktiky
  - ✓ vyžaduje se pro střední úroveň záruky za dosažení bezpečnosti
  - ✓ EAL3 je opřena o důkladné zkoumání TOE (ST, PP)
- Navíc oproti EAL2 se vyžaduje rozsáhlejší testování, kontrola vývojového prostředí a zajištění správy konfigurace
  - ✓ hodnotí se důkazy testování návrhu na vysoké (zdrojové) úrovni
- EAL3 je vhodná pro
  - ✓ podmínky, ve kterých vývojáři nebo uživatelé požadují získání nezávisle vyslovené průměrné úrovně záruky dosažení bezpečnosti a přitom nechtějí provádět rozsáhlý re-engineering
  - ✓ bankovní software pro styk se zákazníky, software CA v PKI, . . .

EALs, Evaluation Assurance Levels, přehled

- *Evaluation assurance level 4 (EAL4) -*
  methodically designed, tested, and reviewed
  - ✓ *EAL4 is applicable in those circumstances where developers or users require a moderate to high level of independently assured security in conventional commodity TOEs and*
  - ✓ *are prepared to incur additional security-specific engineering costs.*

EAL4, metodicky navržený, testovaný a přezkoumaný TOE

- požadavky EAL4 stále umožňují se pohybovat v rámci dobré komerční vývojářské praxe
  - ✓ nevyžadují se podstatné specializované znalosti, dovednosti a jiné zdroje
- EAL4 je nejvyšší úroveň záruk, kterou lze dosáhnout (za rozumné náklady) zpětně, tj. pro již existující produkt
- poskytuje střední až vysokou úroveň záruky nezávisle ověřené záruky za dosažení bezpečnosti pro běžnou komoditu produktů
- vyžaduje ze strany vývojáře nebo uživatelů připravenost k pokrytí dodatečných specifických nákladů spjatých s bezpečnostním inženýrstvím

EAL4, metodicky navržený, testovaný a přezkoumaný TOE

- Navíc oproti EAL3 se vyžaduje pro hodnocení dostupnost
  - ✓ detailního návrhu (low-level design) TOE,
  - ✓ neformálního modelu bezpečnostní politiky TOE a
  - ✓ určité podmnožiny implementace (např. části zdrojového kódu bezpečnostních funkcí)
- Nezávislá analýza zranitelností musí demonstrovat odolnost vůči průniku útočníků s nízkým potenciálem pro útok
- Kontroly vývojového prostředí vyžadují dostupnost
  - ✓ modelu životního cyklu,
  - ✓ stanovení použitých vývojových nástrojů a
  - ✓ automatizovanou správou konfigurace vývojového prostředí
- Novell NetWare, SUSE Linux Enterprise Server 9, Windows 2000 Service Pack 3, Red Hat Enterprise Linux 5

EALs, Evaluation Assurance Levels, přehled

- *Evaluation assurance level 5 (EAL5) -*
  semiformally designed and tested
  - ✓ *EAL5 is applicable in those circumstances where developers or users require a high level of independently assured security in a planned development and*
  - ✓ *require a rigorous development approach without incurring unreasonable costs attributable to specialist security engineering techniques.*

EAL5, semiformálně navržený a testovaný TOE

- vyžaduje se přísné uplatnění dobré komerční vývojářské praxe
  - ✓ aplikace speciálních technik bezpečnostního inženýrství ve středním rozsahu
  - ✓ Daný TOE byl/bude pravděpodobně již navrhovaný a vyvíjený s cílem dosažení úrovně záruk EAL5
  - ✓ Nepředpokládá se nicméně velké zvýšení nákladů oproti EAL4
- EAL5 je vhodná když se vyžaduje nezávisle ověřená vysoká úroveň záruky dosažení bezpečnosti, aniž by náklady na specializované techniky byly nerozumně vysoké
  - ✓ maximálně vysoká úroveň záruky bezpečnosti vyslovitelná na základě zjištění průkazného používaného bezpečnostního konstruování, založeného na dokonalých komerčních vývojových praktikách podporovaných běžnou, nikoli extrémní aplikací speciálních bezpečnostních technik

EAL5, semiformálně navržený a testovaný TOE

- vhodná pro podmínky, ve kterých vývojář nebo uživatel nechtějí hradit neodůvodněně zvýšené náklady na použití speciálních bezpečnostních technik
- Navíc oproti EAL4 je vyžadováno
  - ✓ dodání kompletní implementace TOE,
  - ✓ formální model bezpečnostní politiky TOE,
  - ✓ poloformální presentace funkčních specifikací,
  - ✓ poloformální globální návrh (high-level design) a
  - ✓ poloformální demonstrace korespondence implementace vůči návrhu
- Nezávislá analýza zranitelností musí demonstrovat odolnost vůči průniku útočníků se středním potenciálem pro útok
- Vyžaduje se také analýza skrytých kanálů a modularita návrhu
- čipové karty, některé specializované operační systémy

EALs, Evaluation Assurance Levels, přehled

- *Evaluation assurance level 6 (EAL6) -*
  semiformally verified design and tested
  - ✓ *EAL6 is applicable to the development of security TOEs for application in high risk situations*
  - ✓ *where the value of the protected assets justifies the additional costs.*

EAL6, semif. navržený se semif. ov. návrhem a testovaný

- úroveň záruky dosažení bezpečnosti umožňující vytvářet zvláště propracované produkty nebo systémy IT pro ochranu aktiv s vysokou hodnotou provozované ve vysoce rizikových prostředích
  - ✓ 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
- vyžaduje aplikaci technik bezpečnostního inženýrství do přísného vývojového prostředí
- určena pro vývoj TOE sloužícího pro ochranu vysoce hodnotných aktiv proti význačným rizikům, kdy lze odůvodnit dodatečné náklady

EAL6, semif. navržený se semif. ov. návrhem a testovaný

- Navíc oproti EAL5 se vyžaduje
  - ✓ poloformální detailní návrh,
  - ✓ rozsáhlejší testování,
  - ✓ návrh TOE musí být modulární a vrstvový,
  - ✓ implementace musí být strukturovaná
- Nezávislá analýza zranitelností musí demonstrovat odolnost vůči průniku útočníků s vysokým potenciálem pro útok
- Analýza skrytých kanálů musí být systematická
- Vyšší nároky jsou kladeny na správu konfigurace a na kontrolu vývojového prostředí

EALs, Evaluation Assurance Levels, přehled

- *Evaluation assurance level 7 (EAL7) -*
  formally verified design and tested
  - ✓ *EAL7 is applicable to the development of security TOEs for application in extremely high risk situations and/or where the high value of the assets justifies the higher costs.*
  - ✓ *Practical application of EAL7 is currently limited to TOEs with tightly focused security functionality that is amenable to extensive formal analysis.*

EAL7, form. navržený s form. ov. návrhem a testovaný

- EAL7 je určená pro vývoj bezpečných IT produktů nebo systémů určených pro provozování ve vysoce rizikových prostředích, když vysoká hodnota aktiv ospravedlňuje vynaložení vyšších nákladů
- praktická použitelnost je v současné době omezena na produkty nebo systémy IT s úzce zaměřenou bezpečnostní funkčností, kterou lze rozsáhle analyzovat formálně
- Vyžaduje se
  - ✓ plná formalizace,
  - ✓ formální model bezpečnostní politiky,
  - ✓ formální presentace funkčních specifikací a high-level návrhu,
  - ✓ formální detailní návrh,
  - ✓ poloformální demonstrace korespondence implementace

EAL7, form. navržený s form. ov. návrhem a testovaný

- Testování se vyžaduje na úrovni bílé skříňky (white-box)
  - ✓ testy se definují se znalosti vnitřní struktury
- musí být dosaženo úplného nezávislého potvrzení výsledků všech předložených testů.
- Složitost návrhu musí být minimalizována

Příklad rysů EAL – TOE s EAL 3

- Cíle úrovně záruky EAL 3
  - ✓ dosahuje se maximální jistoty pomocí správně vedeného bezpečnostního inženýrství během návrhu
  - ✓ nezávisle vyslovená záruka za bezpečnost má střední úroveň
  - ✓ TOE a vývoj TOE lze důkladné přezkoumávat bez rozsáhlého, důkladného reengineeringu
- EAL3 poskytuje záruku tím, že
  - ✓ existuje plnohodnotný bezpečnostní cíl, *Security Target (ST)* a
  - ✓ pro porozumění bezpečného chování byla provedena analýza bezpečnostních vlastností (SFR) v bezpečnostním cíli pomocí
    - specifikací funkcí a rozhraní TOE
    - návodů k použití a provozování TOE a
    - popisu architektury TOE

Příklad rysů EAL – TOE s EAL 3

- Analýza je podpořena
  - ✓ nezávislým testováním funkčnosti TOE (TSF, *TOE Security Function*)
  - ✓ důkazy testování provedeného vývojářem na základě specifikace TSF a návrhu TOE
  - ✓ selektivním nezávislým potvrzením výsledků testů provedených vývojářem
  - ✓ analýzou zranitelnosti
- Záruka je dále daná
  - ✓ aplikací bezpečnostních opatření ve vývojovém prostředí
  - ✓ důkazy bezpečných dodavatelských procedur

Příklad rysů EAL – EAL 3, Popis bezpečnostní architektury

- Povinosti vývojáře
  - ✓ TOE je navržený a implementovaný tak, že bezpečnostní vlastnosti TFS nelze obejít
  - ✓ TSF je navržená a implementovaná tak, že je schopná sama sebe chránit před nedovolenými zásahy nedůvěryhodných aktivní subjektů
  - ✓ poskytnout popis bezpečnoostní architektury TSF
- Popis bezpečnostní architektury musí
  - ✓ být vypracovaný na úrovni podrobnosti srovnatelné s popisem abstrakcí SFR popsaných v dokumenetu návrhu TOE
  - ✓ popsat bezpečnostní domény udržované funkcemi TOE konzistentně s bezpečnostními vlastnostmi, SFR
  - ✓ popsat bezpečnost inicializace funkcí TOE
  - ✓ demonstrovat, že funkce TOE chrání sama sebe před narušením
  - ✓ demonstrovat, že funkce TOE zamezují obcházení bezpečnostních vlastnosti

Příklad rysů EAL – EAL 3, Popis bezpečnostní architektury

- Hodnotitel musí
  - ✓ potvrdit, že všechny poskytnuté informace splňují všechny požadavky na obsah a formu důkazu

Příklad rysů EAL – EAL 3, Funkční specifikace

- Vývojář musí
  - ✓ vypracovat funkční specifikaci
  - ✓ dokumentovat cestu od funkční specifikace k bezp. vlastnostem
- Funkční specifikace musí
  - ✓ plně reprezentovat funkce TOE
  - ✓ popsat účel a metody použití všech rozhraní funkcí TOE
  - ✓ identifikovat a popsat všechny parametry všech rozhraní funkcí TOE
  - ✓ popsat akce prosazující bezpečnostní vlastnosti každého rozhraní funkcí TOE
  - ✓ popsat chybové zprávy generované účinky prosazování bezpečnosti a výskytem výjimek souvisejících s vyvoláváním rozhraní funkcí TOE
  - ✓ stručně popsat činnosti rozhraní funkcí TOE nesouvisejících s bezpečností
  - ✓ demonstrovat, jak bezpečnostní vlastnosti souvisí s rozhraním funkcí TOE ve funkční specifikaci

Příklad rysů EAL – EAL 3, Funkční specifikace

- Hodnotitel musí
  - ✓ potvrdit, že poskytnuté informace splňují všechny požadavky na obsah a formu důkazů
  - ✓ vydat rozhodnutí, že funkční specifikace jsou přesné a úplné instalace bezpečnostních vlastnosti, SFR

Příklad rysů EAL – EAL 3, Návrh architektury

- Vývojář musí
  - ✓ Poskytnout návrh TOE
  - ✓ Poskytnout mapování rozhraní funkcí TOE z funkční specifikace na nejnižší úroveň dekompozice použité v návrhu TOE
- Návrh musí
  - ✓ popisovat strukturu TOE v pojmech podsystémů
  - ✓ identifikovat všechny podsystémy funkcí TOE
  - ✓ popsat chování každé samostatného subsystému funkčnosti TOE, který neinterferuje s bezpečnostními vlastnostmi dostatečně podrobně k určení, že bezpečnostní vlastnosti neovlivňuje
  - ✓ popsat chování podporující bezpečnostní vlastnosti subsystémů podporujících bezpečnostní vlastnosti
  - ✓ stručně popsat chování nepodporující bezpečnostní vlastnosti subsystémů podporujících bezpečnostní vlastnosti

Příklad rysů EAL – EAL 3, Návrh architektury

- ✓ stručně popsat chování subsystémů podporujících bezpečnostní vlastnosti
- ✓ poskytnout popis interakcí mezi všemi podsystémy funkčnosti TOE
- ✓ demonstrovat, že všechna chování popsaná v návrhu TOE jsou mapována na rozhraní funkcí TOE, která je vyvolávají

□ Hodnotitel musí

- ✓ potvrdit, že poskytnuté informace splňují všechny požadavky na obsah a formu důkazů
- ✓ vydat rozhodnutí, že návrh je přesnou a úplnou instalace bezpečnostních vlastnosti, SFR

Příklad rysů EAL – EAL 3, Provozní dokumentace

- Vývojář musí poskytnout provozní dokumentaci
- Provozní dokumentace musí
  - ✓ popsat pro každou uživatelskou roli, uživatelům dostupných funkcí a oprávnění, které mají být řízené v prostředí bezpečného provozování, včetně odpovídajících varování
  - ✓ popsat pro každou roli uživatele jak se bezpečným způsobem používají dostupná rozhraní poskytované TOE
  - ✓ popsat pro každou roli uživatele dostupné funkce a rozhraní, zejména všechny bezpečnostní parametry zadávané uživatelem, vč. indikací vhodných bezpečných hodnot
  - ✓ pro každou uživatelskou roli uživatele jasně prezentovat každý typ bezpečnostní události související s funkcemi dostupnými uživateli, které je třeba provést, včetně změn bezpečnostních charakteristik prvků ovládaných funkčností TOE

Příklad rysů EAL – EAL 3, Provozní dokumentace

- ✓ identifikovat všechny možné režimy provozování TOE (včetně provozu po výpadku nebo provozní chybě), jejich dopady a důsledky pro zachování bezpečného provozu
- ✓ pro každou uživatelskou roli uživatele popsat bezpečnostní opatření, která je třeba dodržovat, aby naplnily bezpečnostní cíle pro provozní prostředí popsané v bezpečnostním cíli, ST
- ✓ být srozumitelně napsaná a přiměřeně rozsáhlá

□ Hodnotitel musí

- ✓ potvrdit, že poskytnuté informace splňují všechny požadavky na obsah a formu důkazů

Příklad rysů EAL – EAL 3, Instalační procedury

- Vývojář musí
  - ✓ poskytnout TOE vč. instalačních procedur
- Přípravné procedury musí
  - ✓ popsat všechny kroky nezbytné pro bezpečné převzetí dodaného TOE v souladu s procedurami dodávky od vývojáře
  - ✓ popsat všechny kroky nezbytné pro bezpečnou instalaci TOE a pro bezpečnou přípravu provozního prostředí v souladu s bezpečnostními cíli pro provozní prostředí popsáné v bezpečnostním cíli, ST
- Hodnotitel musí
  - ✓ potvrdit, že poskytnuté informace splňují všechny požadavky na obsah a formu důkazů
  - ✓ použít instalační postupy aby potvrdil, že TOE lze připravit na provoz bezpečně