Kritéria hodnocení informační bezpečnosti

PV 017 ◇ Bezpečnost IT

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

Verze : podzim 2019

Motivace pro použití hodnotících nástrojů

- Je dostupný aplikační produkt (sytém) deklarující odolnost vůči jistým hrozbám vůči informační bezpečnosti
  - ✓ sestává z software, firmware a/nebo hardware a případně jsou dostupné i návody k použití
  - ✓ deklaruje se, že zajišťuje integritu, důvěrnost, dostupnost, ... při plnění jím poskytovaných služeb
  - ✓ deklaruje se, že tyto vlastnosti zajišťuje vůči silným útokům
- Jak ověřit zda jsou deklarace důvěryhodné ?
  - ✓ třetí nezávislá strana provede hodnocením vlastností produktu (systému) a potvrdí, že deklarace jsou validní
    - potvrzení důvěryhodnosti může mít formu auditní (hodnotící) zprávy
    - důvěryhodnější formou potvrzení je získání certifikátu vydaného důvěryhodnou certifikační autoritou

Předmět hodnocení

- Předmětem hodnocení (*Target of Evaluation*, TOE) může být IT produkt, část IT produktu, sestava IT produktů, ...
  - ✓ Softwarová aplikace (SA), OS, kombinace SA s OS, kombinace SA/OS a HW platformy, databáze, LAN vč. aplikací, integrovaný obvod pro smart karty, ...
  - ✓ Pokud se předmět hodnocení může vyskytovat ve více konfiguracích, musí se definovat, která z nich je TOE
  - ✓ IS řešící personalistiku a mzdy
- TOE rovněž může mít charakter systému implementovaného a provozovaného konglomerátu produktů v konkrétním kontextu
  - ✓ IS řešící personalistiku a mzdy v konkrétní organizaci

Motivace pro použití hodnotících nástrojů

- Čím je daná síla záruky za to, že deklarace vlastností TOE jsou validní ?
  - ✓ Síla záruky se přirozeně odvozuje od důslednosti, detailnosti, přesnosti, důkladnosti, ... provedeného hodnocení jak byl TOE navržený, implementovaný, zda byly aplikovány potřebné zásady bezpečnostního inženýringu, ...
  - ✓ Cena za získání záruky je minimálně přímo úměrná požadované síle záruky, cena získání záruky obvykle roste rychleji než síla záruky
- Jak silná záruka za důvěryhodnost vlastností TOE je nutná ?
  - ✓ Potřebná síla záruky je dána potenciálem možných škod způsobených provozováním produktu (systému)
  - ✓ Pro systém řešící běžnou provozní agendu organizace pravděpodobně vystavený pouze běžným slabým útoků stačí slabší záruka než pro systém zpracovávající vysoce citlivá data s potenciálem silných útoků (např. systém elektronického bankovnictví)

Škálování síly záruky

- Pozitivní výsledek hodnocení získaný ověřením bezpečnostních vlastností TOE opravňuje vyslovit
  - ✓ velmi nízkou záruku,
    pokud hodnocení bylo provedené
    pouze na základě testů vůči uživatelskému manuálu TOE
  - ✓ nízkou záruku,
    pokud pro hodnocení se navíc použila
    neformální specifikace bezpečnostních vlastností TOE
  - ✓ středně silnou záruku,
    pokud se při hodnocení použila semi-formální specifikace, zkoumal se
    detailní návrh a zdrojové kódy programů, logická schémata . . . TOE
  - ✓ velmi silnou záruku,
    pokud se pro hodnocení použila
    plně formální specifikace vlastností (algebraicko-logický model)
    a pokud se při hodnocení formálně prokázala validnost a
    návaznost návrhu, detailního návrhu a implementace TOE

Motivace pro použití standardních hodnotících nástrojů

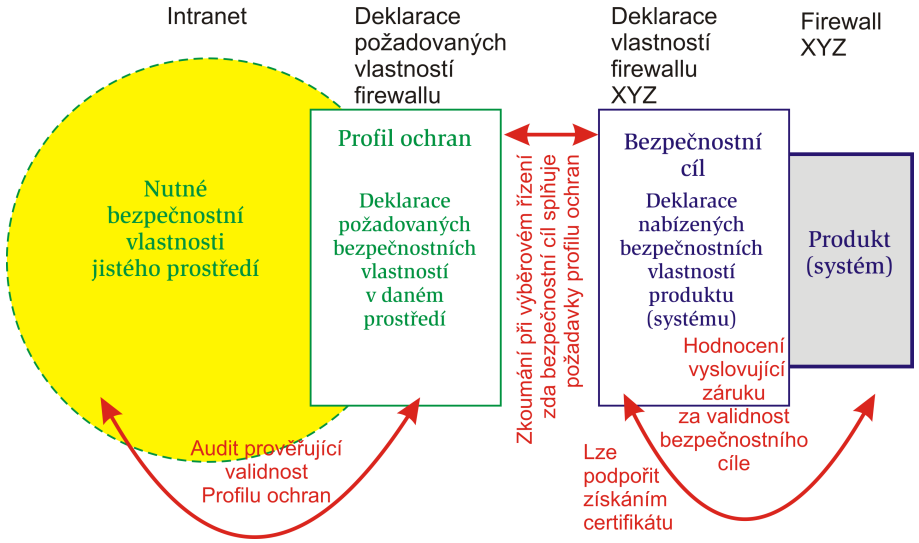
- Aby byla deklarovaná záruka za validnost bezpečnostních vlastností TOE důvěryhodná, musí se vyslovit na základě standardizovaného, všeobecně uznávaného, reprodukovatelného, opakovatelného šetření
  - ✓ Deklarovaná záruka musí být přesným výsledkem šetření,
    opakování či reprodukce šetření musí dát stejný výsledek
  - ✓ opakovatelnost (měření, auditu, . . .)
    aplikuje se stejný postup šetření, stejnými šetřícími nástroji,
    ve stejném pracovním prostředí, stejného TOE
  - ✓ reprodukovatelnost (měření, auditu, . . .)
    aplikuje se stejný postup šetření, stejnými šetřícími nástroji,
    v podobném pracovním prostředí na jiném TOE téhož typu TOE
- Takové šetření specifikuje standard

  ISO/IEC 15408, Evaluation criteria for IT security

Poznání zásad a principů ISO/IEC 15408 je cílem přednášky

- Standard řeší jak zadat při poptávce / výběrovém řízení
  požadovanou bezpečnostní funkčnost produktu/systému a
  požadovanou úroveň záruky za její validnost
  (deklarací profilu ochran,
  kterému musí produkt/systém vyhovovat)
- Standard rovněž řeší jak deklarovat
  bezpečnostní funkčnost nabízeného produktu/systému a
  úroveň záruky za validnost této funkčnosti
  (deklarací bezpečnostního cíle produktu/systému)
- Standard definuje obsah
  nezávislého šetření splnění požadavků na zaručitelnost za
  dosažení informační bezpečnosti
  odpovídajících udané síle zaručitelnosti

Cíl přednášky – poznání zásad a principů ISO/IEC 15408



ISO/IEC 15408, Evaluation criteria for IT security

- standard původně zvaný Common Criteria, CC
  vydaný ISO/IEC/JTC1/SC 27/WG3
- Skladba standardu – 3 části
  - ✓ ISO/IEC 15408-1: Part 1: Introduction and general model
  - ✓ ISO/IEC 15408-2: Part 2: Security functional components

    sbírka vzorů (šablon) požadavků na bezpečnostní funkčnosti TOE, které jsou nutné pro splnění bezpečnostních cílů TOE.

    Definice bezpečného chování TOE (z pohledu identifikace, autentizace, nepopiratelnosti, ...) se provádí výčtem požadavků na škálu plněných bezpečnostních funkcí (opatření, ...):

    User identification (FIA_UID)
    Confidentiality of imported data (FCO_CID)
    Random number generation (FMI_RND) ... ...

    Bezpečnostní funkčnost TOE vzniká implementací těchto požadavků na bezpečnostní funkčnost

ISO/IEC 15408, Evaluation criteria for IT security

- ✓ ISO/IEC 15408-3: Part 3: Security assurance components

  sbírka komponent – vzorů (šablon) požadavků na zaručitelnost validní bezpečnostní funkčnosti TOE.

  Popisy toho, co se má hodnotit podle požadované síly záruky za validnost bezpečnostní funkčnosti TOE:

  provedení analýzy zranitelnosti,
  použití konfiguračních procedur,
  procedury správy vývojového prostředí, ...)

  Definují se dokumenty Profil ochran a Bezpečnostní cíl TOE.

  Prezentuje se sedm předdefinovaných balíčků požadavků na zaručitelnost nazývaných Evaluation Assurance Levels (EALs).

- všechny 3 části byly po prvé publikované v r. 2005, zatím poslední revize v r. 2014

ISO/IEC 15408 jsou hodnotící kritéria

- Hodnotící kritéria podporují vyslovení záruky, že procesy
  – specifikace informační bezpečnosti TOE,
  – implementace informační bezpečnosti TOE a
  – a vlastního hodnocení informační bezpečnosti TOE
  byly vedené přísným a standardním způsobem
- Hodnotící kritéria =
  - ✓ seznam podmínek, které vyvíjený/kupovaný produkt nebo systém má být schopný (musí) splnit, resp. kterým musí vyhovět
- Hodnotící kritéria $\neq$ metodologie hodnocení
  - ✓ metodologie hodnocení = způsob provedení hodnocení zda hodnocený produkt/systém vyhovuje stanoveným kritériím
  - ✓ metodologii obvykle určuje autorita, která je v dané oblasti (např. EU, stát, koncern, ...) odpovědná za dodržování konzistence hodnocení

Kdo standard hodnotících kritérií IT bezpečnosti využívá ?

- ISO/IEC 15408 poskytuje prostředí (*framework*), ve kterém
  – zákazník může udat požadavky na informační bezpečnost požadovaného produktu/systému a žádanou sílu záruky za jejich validnost
  – výrobce může specifikovat bezpečnostní vlastnosti nabízeného produktu/systému
  – hodnotitel může hodnotit, zda daný TOE má deklarované vlastnosti
- Zákazník
  - ✓ při vypisování výběrového řízení zadává požadavky na bezpečnostní vlastnosti požadovaného informačního systému (produktu) – vydává profil ochran, které musí nabízený produkt poskytovat
  - ✓ Výsledky hodnocení bezpečnostního cíle TOE mu sdělují, zda bezpečnostní vlastnosti TOE odpovídají jeho představám

Kdo standard hodnotících kritérií IT bezpečnosti využívá ?

- Vývojář
  - ✓ jako vodítko pro plánování bezpečnostních vlastností vyvíjeného produktu resp. systému
  - ✓ bezpečnostní vlastnosti vyvíjeného produktu/systému deklaruje jeho bezpečnostní cíl
  - ✓ bezpečnostní cíl může vyhovovat požadavkům jednoho nebo i více profilů ochran

Kdo standard hodnotících kritérií IT bezpečnosti využívá ?

- Hodnotitel –
  - ✓ jako programový profil svých činností
  - ✓ hodnocení se vesměs řeší jako zakázková činnost, hodnotitel = firma
  - ✓ mezi typické činnosti vykonávané hodnotitelem patří:
    - potvrzení, že daný profil ochran odpovídá požadavkům zákazníka
    - potvrzení, že bezpečnostní vlastnosti TOE odpovídají vlastnostem deklarovaným v jeho bezpečnostním cíli
    - potvrzení,že jistý bezpečnostní cíl vyhovuje požadavkům deklarovaným daným profilem ochran
  - ✓ fakt, že hodnotitel pro hodnocení prokazatelně používá správná kritéria a správnou metodologii hodnocení může potvrzovat certifikátem relevantní autorita pro hodnocení informační bezpečnosti
  - ✓ na základě hodnotitelské zprávy TOE může vydat certifikát potvrzující záruku za bezpečnostní vlastnosti TOE certifikační autorita

Hodnotící kritéria a standardy kritérií vývoje IT bezpečnosti

- Hodnotící kritéria ≠ standardy vývoje produktu/systému splňujícího požadavky standardů rodiny ISO/IEC 27000
  - ✓ i když lze standardy ISO/IEC 27001 a ISO/IEC 27002 použít pro hodnocení jak se zachází s informacemi, není to jejich cílem,
    - jsou příliš technicky orientované
    - jejich smyslem je definovat, jak bezpečně manipulovat s informacemi
  - ✓ ani ISO/IEC 27001 ani ISO/IEC 27002 nepožadují použití
    - hodnocených produktů, resp.
    - produktů s certifikátem dosažené úrovně informační bezpečnosti
  - ✓ ISO/IEC 27001 i ISO/IEC 27002 pouze požadují,
    - aby produkt / systém byl externě auditovatelný a
    - aby se pravidelně kontroloval soulad jeho bezpečnostních vlastností systému s vhodnými implementačními kritérii, kterými mohou být např. hodnotící kritéria

Vyslovení záruky bezpečnosti informací v produktu/systému

- Cíl hodnocení z pohledu bezpečnosti informací
  - ✓ vyslovení úrovně záruky, s jakou lze garantovat, že produkt/systém zajišťuje (deklarovanou) informační bezpečnost
  - ✓ Použitá hodnotící kritéria proto musí definovat míru záruky
  - ✓ Míra záruky musí být vyjádřená vhodnými stupni (úrovněmi)
    - obecně, např.: nízká, střední, vysoká, . . .
    - podle CC: EAL1, EAL2, . . . , EAL7 , EAL – Evaluation Assurance Level,

      EALi = úroveň záruky za dosaženou kvalitu informační bezpečnosti,

      POZOR: nikoli síly použitých bezpečnostních mechanismů, hodnotí se kvalita specifikace, implementace, dodávek, . . .

      EAL1 – nejnižší záruka kvality informační bezpečnosti

      . . .

      EAL7 – nejvyšší záruka kvality informační bezpečnosti

Vyslovení záruky bezpečnosti informací v produktu/systému

- Pro dosažení cíle hodnocení – tj. pro vyslovení záruky
  za dosaženou kvalitu informační bezpečnosti,
  se musí prokázat, že zavedená bezpečnostní opatření
  - ✓ mají správnou funkčnost,
    ≡ poskytují ochranu proti všem relevantním hrozbám
  - ✓ jsou efektivní,
    ≡ účinně zabraňují hrozbám, kvůli kterým byly zavedeny
  - ✓ Hloubka a důkladnost procedur ověření obou těchto deklarovaných vlastností jsou dané udanou/požadovanou úrovní záruky,
    pro EAL1 se ověřují na základě uživatelské dokumentace
    pro EAL7 se ověřují na precizních algebraicko-logických modelech
    POZOR – nemůžeme si být nikdy jisti
    absolutní efektivitou a
    perfektní funkčností prosazovaných opatření

Produkt, systém, předmět hodnocení

- Hodnocení produktu
  - ✓ obtížně se posuzuje efektivnost bezpečnostních rysů,
    – nebývá známé prostředí, ve kterém bude produkt provozovaný
    – není jasné, co bude konkrétní uživatel od produktu požadovat,
  - ✓ při návrhu vlastností produktu se musí brát do úvahy generické požadavky většiny uživatelů
  - ✓ je odpovědností hodnotitele, jak kontroluje funkčnost a efektivitu
- Hodnocení systému
  - ✓ požadavky na efektivnost bezpečnostních rysů systému bývají zřejmé,
    – známe prostředí, ve kterém bude systém provozovaný
    – je jasné, co konkrétní uživatel od produktu požaduje
  - ✓ jejich vyslovení je ale složitý a technický proces

Přínosy a problémy hodnocení

- Přínosy hodnocení pro podnikání
  - ✓ provedení hodnocení může produktu otevřít cestu na nové trhy (např. do oblasti státní správy, zdravotnictví, armády, . . .)
  - ✓ hodnocení může odstranit starost, zda produkt má šanci uspět na trhu
  - ✓ výsledek hodnocení obecně bývá dobrý reklamní nástroj
- Problémy s hodnocením
  - ✓ jakákoliv změna TOE (např. záplatou) hodnocení znehodnocuje až anuluje
  - ✓ uživatel, který není expertem v (hodnocení) bezpečnosti
    – nemusí plně rozumět zárukám odvozeným z výsledků hodnocení a
    – nemusí být schopný zadat požadavky na hodnocení

Kdo hradí hodnocení ?

- Náklady hodnotiteli vždy hradí sponzor hodnocení
  - ✓ výrobce produktu
  - ✓ vlastník systému
- Při volbě cílové úrovně záruky hraje důležitou roli cena hodnocení
- Je-li TOE produkt, náklady na hodnocení lze rozptýlit mezi velký počet zákazníků
- Je-li TOE systém, veškeré náklady hradí vlastník systému

Metodologie hodnocení

- Hodnocení provádí hodnotitel
- Hodnotitel má být dozorovaný (kontrolovaný, prověřovaný) autoritou pro hodnocení informační bezpečnosti
- pro sponzora hodnocení je hodnotitel důvěryhodnou třetí stranou
  - ✓ Použití takových partnerů mj. požaduje i standard ISO/IEC 27002
- Sponzor hodnocení uzavírá s hodnotitelem smluvní vztah
- Každá fáze hodnocení vyjmenovaná ve smlouvě probíhá podle definovaných postupů vč. definovaného harmonogramu
- Hodnotitel vypracovává hodnotící zprávu, ve které vyslovuje důkazy podepřené závěry o kvalitativní úrovni bezpečnostních vlastností TOE

Metodologie hodnocení

- Ve smlouvě se vymezuje zda hodnotící zpráva bude důkazem pro vydání certifikátu dosažené úrovně záruky za kvalitu informační bezpečnosti
- Certifikát dosažené úrovně záruky odvozené při hodnocení vydává uznávaná certifikační autorita na základě hodnotící zprávy hodnotitele
- Certifikační autority bývají licencované komerční organizace licencované = akreditované u relevantní autority

Metodologie hodnocení

- Autoritou pro hodnocení informační bezpečnosti IT má být národní / mezinárodní instituce, která kontroluje, že
  - ✓ všichni pod ni spadající hodnotitelé splňují profesní vlastnosti požadované od hodnotitelů
  - ✓ všechny pod ni spadající certifikační autority splňují profesní vlastnosti požadované po certifikačních autoritách
  - ✓ Hodnotitelé a certifikační autority se musí obvykle ucházet o akreditaci u takové autority pro hodnocení bezpečnosti IT

Investigace nebo audit ?

- Metody hodnocení mohou být
  - ✓ produktově/systémově orientované, investigativní hodnocení
    - zkoumá se, testuje se, hotový produkt/systém a jeho vlastnosti
    - hodnocení je obtížně opakovatelné, je individuální pro každý TOE
  - ✓ procesně orientované, auditní postup
    - hodnotí se dokumentace a procesy návrhu, vývoje, pořizování a provozování TOE
    - levnější a snadněji opakovatelné hodnocení, avšak pro koncového uživatele může být méně užitečné
    - přesto upřednostňovaná forma, uplatněná i v ISO/IEC 15408

Specifikační dokument CC, Protection Profile

- profil ochran, *Protection Profile*, PP
  - ✓ dokument typicky vytvářený uživatelem nebo nějakou uživatelskou komunitou
  - ✓ identifikuje požadavky na bezpečnost pro jisté prostředí
    - použití čipových karet pro dosažení nepopiratelnosti (podpisování)
    - síťové firewally (pro řízení přístupu), ...
  - ✓ výrobce se může rozhodnout vyrábět zařízení vyhovující konkrétnímu PP,
  - ✓ výrobek lze certifikovat jako vyhovující PP
  - ✓ PP lze použít jako šablonu pro definici bezpečnostního cíle (specifikaci bezpečnostních vlastností konkrétního produktu/systému)
  - ✓ zákazník si může vybírat z produktů, které deklarují vyhovění jistému PP, resp. které vlastní certifikát vyhovění jistému PP

Specifikační dokument CC, Security Target

- bezpečnostní cíl, *Security Target*, ST
  - ✓ dokument definující bezpečnostní vlastnosti produktu/systému, tzv. Security Functional Requirements (SFRs)
    - specifikace bezpečnostních funkcí poskytovaných produktem
    - součástí CC je standardní katalog těchto funkcí
    - např SFR může definovat, jak se má konkrétní role autentizovat
    - CC nepředpisují žádné povinné SFR v ST
    - některé SFR se mohou podmiňovat – např. schopnost omezovat přístup rolím vyžaduje nutnost mít možnost identifikovat jednotlivé role
  - ✓ produkt/systém se obvykle hodnotí jak splňuje zadaný/deklarovaný ST, – je hodnocený proti SFRs deklarovaným v ST
  - ✓ lze rovněž hodnotit ST, zda vyhovuje zadanému PP
  - ✓ ST je mnohdy reklamním materiálem výrobce

Specifikační dokument CC, Security Target

- ST obsahuje popisy bezpečnostních problémů řešených pomocí TOE a provozního prostředí TOE
  - ✓ TOE zákazníkovi vyhovuje,
    - pokud se shoduje zákazníkův bezpečnostní problém s problémem, o kterém se v ST daného TOE říká, že je tímto TOE řešený, a
    - pokud se shoduje provozní prostředí zákazníka s prostředím, ve kterém musí být TOE provozovaný
- TOE lze hodnotit proti ST, hodnotí se jak TOE splňuje ST
- ST může deklarovat, kterým PP vyhovuje a TOE pak lze hodnotit i proti těmto PP, zda jim provozní prostředí TOE odpovídá
  - ✓ Zákazník může deklarovat, který PP charakterizuje jeho provozní prostředí a jeho bezpečnostní problémy

Common Criteria, hodnocení produktu a PP

- Hodnocení produktu/systému (TOE) typicky sestává ze 2 kroků
  - ✓ hodnocení ST,
    o kterém TOE sděluje, že ho splňuje, aby se získala jistota, že problém řešený produktem je problémem, který je potřeba řešit
  - ✓ vlastní hodnocení TOE proti tomuto ST, aby se získala jistota, že TOE splňuje úroveň zaručitelnosti definované v ST
- Hodnocení PP
  - ✓ probíhá před formální deklarací PP relevantní autoritou odpovědnou za bezpečnost IT
  - ✓ cílem hodnocení je získání jistoty, že PP správně identifikuje požadavky na bezpečnost

Jak CC používají . . .

- Zadavatelé vývoje
  - ✓ jako specifikace bezpečnostních požadavků na TOE stanovují Profily ochran – dokumenty popisující generické požadavky na bezpečnostní rysy třídy produktů
  - ✓ a případně i Bezpečnostní cíl – požadavky na bezpečnostní vlastnosti konkrétních produktů
- Vývojáři
  - ✓ specifikují bezpečnostní vlastnosti vyvíjeného TOE dokumentem Bezpečnostní cíl, pokud ST nezdal zadavatel vývoje
- Hodnotitelé
  - ✓ používají Profily ochran a Bezpečnostní cíle jako měřítko míry, zda / jak TOE vyhovuje požadované bezpečnosti

Jak CC používají . . .

- Zákazníci (při vypsání výběrového řízení, . . .)
  - ✓ zákazník vyhledá/vypracuje Profil ochrany, který splňuje jeho požadavky a použije ho při specifikaci objednávky, vypsání výběrového řízení, . . .
- Uživatelská sdružení, resorty (zdravotnictví, státní správa, školství, bankovní sektor, . . .)
  - ✓ definují pomocí CC Profily ochran, které specifikují společné/generické požadavky na bezpečnost

Struktura ST/PP

- Úvod
  - ✓ orientační popis řešeného problému na vyjadřovací úrovni běžného uživatele
- Popis zařízení (TOE), prohlášení shody, (TOE DESCRIPTION)
  - ✓ podrobný popis účelu, chování, struktury, . . . vyhovujícího TOE
  - ✓ popis jak ST/PP splňuje Common Criteria a příp. které PP splňuje ST
- Definice bezpečnostního problému (TOE SECURITY ENVIRONMENT)
  - ✓ popis předpokládaných podmínek/vlastností provozního prostředí
  - ✓ popis ošetřovaných hrozeb

Struktura ST/PP

- Bezpečnostní cíle (SECURITY OBJECTIVES)
  - ✓ popis bezpečnostních vlastností TOE, vývojového prostředí a provozního/organizačního prostředí
- Bezpečnostní požadavky (IT Security Requirements)
  - ✓ překlad bezpečnostních cílů do technických požadavků, které musí být splněny
  - ✓ např. – požaduje se, aby veškerý zdrojový kód byl spravovaný správním systémem pro změnové řízení
  - ✓ např. – požaduje se provedení úplného otestování funkčnosti
  - ✓ TOE je hodnocený proti této sekci
  - ✓ hodnotí se ST, aby se získala jistota, že tato sekce odpovídá cílům
- Odůvodnění bezpečnostních cílů (RATIONALE)
- Pro ilustraci – příklady rozsahů typických PP
  - ✓ PP firewallu 60 až 200 stran, PP PKI 150 až 200 stran
  - ✓ sbírka šablon PP viz *http://www.commoncriteriaportal.org/pps/*

Dvě kategorie požadavků na IT bezpečnost dosahovanou TOE

- funkční požadavky – cíle z hlediska bezpečnosti informací
  - ✓ Security Functional Requirements (SFRs)
  - ✓ CO TOE DĚLÁ ? – při hodnocení produktu/systému proti jeho ST, resp. CO TOE MÁ DĚLAT ? – při hodnocení PP/ST
  - ✓ definice bezpečného chování TOE (identifikace, autentizace, nepopiratelnost, ...) se provede výčtem požadavků na škálu poskytovaných bezpečnostních funkcí
  - ✓ bezpečnostní funkce (opatření, ...) vznikají implementací funkčních požadavků

Dvě kategorie požadavků na IT bezpečnost dosahovanou TOE

- požadavky dané stanovenou úrovní zaručitelnosti za kvalitu, validnost bezpečnostní funkce
  - ✓ Security Assurance Requirements
  - ✓ JE TOE UDĚLÁN DOBŘE A DĚLÁ CO MÁ DĚLAT ?
  - ✓ určeno pro stanovení velikosti důvěry v bezpečnostní funkce vytvořené implementací funkčních požadavků
  - ✓ síla záruky se odvozuje z důkazů získaných prokázáním správnosti návrhu a implementace tj. účinného splnění cílů, což vyžaduje dostupnost specifikace
    - síly (odolnosti, účinnosti, ...) bezpečnostních funkcí
    - důkazů, které musí poskytnout vývojář
    - důkazů, které musí vypracovat hodnotitel
    - rozsahu (hloubky, přísnosti, ...) hodnocení

Požadavky na bezpečnostní funkčnost

- Security Functional Requirements (SFRs)
- Popis možných požadavků na bezpečnostní funkčnost uvádí část II kritérií
- Popis možných ... = které bezpečnostní funkce lze poskytovat
- 44 požadavků na funkčnost seskupených do 6 tříd
- mohou být zahrnuty mezi Bezpečnostní požadavky v ST/PP
- Příklady
  - ✓ User identification (FIA_UID)
  - ✓ Confidentiality of imported data (FCO_CID)
  - ✓ Random number generation (FMI_RND)
  - ✓ ...

Požadavky na bezpečnostní funkčnost

- Jedná se o definice kritérií pro stanovení/hodnocení profilů ochrany (PP) a bezpečnostních cílů (ST) z hlediska funkčností v oblastech
  - ✓ Security Audit
  - ✓ Communication
  - ✓ Cryptographic Support
  - ✓ User Data Protection
  - ✓ Identification and Authentication
  - ✓ Security Management
  - ✓ Privacy
  - ✓ Protection of the TSF
  - ✓ Resource Utilization
  - ✓ TOE Access
  - ✓ Trusted path/channels

Požadavky na záruku dosažení bezpečnosti

- Security Assurance Requirements
- Popis, jak spolehlivě se mají SFR implementovat obsahuje část III kritérií
  - ✓ výčtové seznamy pro vývojáře/hodnotitele, uvádějí se v ST a v PP
  - ✓ popisy opatření přijímaných během vývoje/hodnocení produktu s cílem vyhovění/prokázání deklarované bezpečnostní funkčnosti
  - ✓ např. – požaduje se, aby veškerý zdrojový kód byl spravovaný správním systémem pro změnové řízení
  - ✓ např. – požaduje se provedení úplného otestování funkčnosti
- úroveň splnění požadavků na záruku deteriminuje zařazení TOE na konkrétní úroveň záruky, *Evaluation Assurance Level* (EAL) – *1, 2, . . . , 7*
  - ✓ tvrdost, přísnost splnění a hodnocení požadavků je dáno EAL zvyšuje se a rozšiřuje se se vzrůstem čísla EAL

Požadavky na záruku dosažení bezpečnosti

- Jedná se o definice kritérií pro stanovení/hodnocení profilů ochrany (PP) a bezpečnostních cílů (ST) z hledisek
  - ✓ Configuration Management / Správy konfigurace
  - ✓ Guidance Documents / Průvodní dokumentace
  - ✓ Vulnerability Assessment / Posouzení zranitelnosti
  - ✓ Delivery and Operation / Dodání a provozu
  - ✓ Life Cycle Support / Podpory životního cyklu
  - ✓ Assurance Maintenance / Zajišťování údržby
  - ✓ Development / Vývoje
  - ✓ Tests / Testování

Úrovně záruky dosažení bezpečnosti

- numerické škálování podle dosaženého plnění různě silných požadavků na bezpečnost
- škála – množina úrovní záruky EAL0 až EAL7
- každé EAL odpovídá balík požadavků na záruku bezpečnosti
- tento balík pokrývá požadavky na přísnost vývoje, kvalitu dokumentace, zajištěnost provozu, . . . TOE
  - ✓ EAL0 – chybný / nehodnotitelný TOE
  - ✓ EAL1 – funkčně správný TOE, nevystavený velkým hrozbám
  - ✓ . . .
  - ✓ EAL4 – funkčně i strukturálně správný TOE, vystavený silným útokům
  - ✓ . . .

Úrovně záruky dosažení bezpečnosti

- vyšší EAL obecně neimplikuje ,,vyšší bezpečí",
- vyšší EAL pouze indikuje,že daný TOE je důvěryhodnější

Úrovně záruky dosažení bezpečnosti

- Balík požadavků na záruku dosažení bezpečnosti dávaný do ST/PP se nevolí ad hoc, obvykle se přebírá se z definice určené cílové EAL

Příklad vztahu záruky dosažení bezpečnosti a EAL:

- ALC_DVS, *Assurance – Life cycle support, Development security*
- rodina záruk ALC_DVS obsahuje 2 úrovně záruk:
  - ✓ ALC_DVS.1: ve vývojovém prostředí existují dobré správní procedury
  - ✓ ALC_DVS.2: platí ALC_DVS.1 a existuje důkaz, že tyto proceduru pro ochranu TOE dostačují
- TOE deklarující v ST/PP úrovně záruky
  - ✓ EAL1 nebo EAL2 nemusí demonstrovat splnění žádné záruky ALC_DVS
  - ✓ EAL3, EAL4 nebo EAL5 musí demonstrovat splnění záruky ALC_DVS.1
  - ✓ EAL6 nebo EAL7 musí demonstrovat splnění záruky ALC_DVS.2

Mezinárodní uznávání

- Pro komerční životaschopnost hodnocení je nutné, aby bylo uznáváno v co nejširším obchodním prostoru
- Hodnotící autority musí souhlasit s uznáváním certifikátů vydaných hodnotícími centry, která pod ně nespadají
- 22 zemí uznává *Common criteria recognition arrangement* (CCRA), které toto uznávání garantuje
- Stránky vybraných institucí oprávněných k vydávání certifikátů IT v rámci CCRA splňujících národní schémata pro hodnocení a certifikaci IT podle CC, :
  - ✓ UK, *http://www.cesg.gov.uk/site/iacs/index.cfm*
  - ✓ USA, *http://niap.nist.gov/cc-scheme*
  - ✓ Německo, *http://www.bsi.bund.de*
  - ✓ CZ, NBU – certifikáty uznává, žádná organizace v CZ je zatím nevydává

EALs, Evaluation Assurance Levels, přehled

- úrovně záruky za dosažení informační bezpečnosti v TOE
- 7 definovaných úrovní záruky za dosažení informační bezpečnosti v TOE (přibližný ekvivalent dle TCSEC)
  - ✓ EAL1, funkčně testovaný TOE
  - ✓ EAL2, strukturálně testovaný TOE (∼ TCSEC C1)
  - ✓ EAL3, metodicky testovaný a kontrolovaný TOE (∼ TCSEC C2)
  - ✓ EAL4, metodicky navržený, testovaný a přezkoumaný TOE (∼ TCSEC B1)
  - ✓ EAL5, semiformálně navržený a testovaný TOE (∼ TCSEC B2)
  - ✓ EAL6, semiformálně navržený se semiformálně ověřeným návrhem a testovaný TOE (∼ TCSEC B3)
  - ✓ EAL7, formálně navržený s formálně ověřeným návrhem a testovaný TOE (∼ TCSEC A1)

Implikace z úrovní záruk

- s růstem čísla EAL se zvyšuje úplnost a přísnost hodnocení dosažené kvality plnění požadavků na bezpečnost
  - ✓ nic více, nic méně
  - ✓ vyší číslo EAL neznamená dosažení vyššího bezpečí, silnější mechanismy apod.
- cenové orientační pohledy (USA, před pár lety)
  - ✓ EAL2: 80 000 – 200 000 USD, 5 – 10 měsíců
  - ✓ EAL3: 100 000 – 250 000 USD, 6 – 12 měsíců
  - ✓ EAL4: 150 000 – 350 000 USD, 8 – 24 měsíců

Která EAL je vhodná pro náš TOE ?

- Standard CC neposkytuje metodologii, návod, pro rozhodnutí, která EAL je nejvhodnější pro daný TOE
  - ✓ Relevantní míry jsou stále předmětem vývoje / výzkumu
  - ✓ Požadovanou EAL má určit zákazník, zákazník vlastní aktiva, prodejce nemůže znát hodnotu/rizika kritických aktiv zákazníka

Která EAL je vhodná pro náš TOE ?

- Čím se liší EAL ?
  - ✓ EAL1 → EAL 7
    rostou požadavky na kvalitu vývojového procesu TOE
  - ✓ EAL1 → EAL 7
    rostou požadavky na rozsah *white-box* testování TOE
  - ✓ EAL1 → EAL 7
    roste potenciál útoku na provoz TOE, výší škod, silou útočníků

    EAL1–EAL3: odolnost vůči slabým útokům, nízká až střední výše škod
    EAL4: odolnost vůči běžným útokům, střední škody
    EAL5: odolnost vůči silným útokům, velké škody
    EAL6 – EAL7: odolnost vůči extrémně silným útokům profesionálů
  - ✓ Důležitou roli hraje zbytková zranitelnost TOE, př. EAL3:

    This TOE may not be resistant to MODERATE and HIGH level attack potential. This TOE may include vulnerability that will be exploitable by attackers who have MODERATE or HIGH level attack potential.

Která EAL je vhodná pro náš TOE ? Příklad řešení

- Máme chránit aktiva v systému proti neautorizovanému zpřístupnění (*C, confidentiality*), neautorizované modifikaci (*I, integrity*) a ztrátě dostupnosti (*A, availability*) aktiva
- Útoky na jednotlivá aktiva v systému mohou způsobit škody škálované do škodních tříd následovně
  - ✓ C: žádná, nízká, střední, vysoká škoda (numericky 0, 1, 2, 3)
  - ✓ I: nízká, střední, vysoká škoda (numericky 1, 2, 3)
  - ✓ A: nízká, střední, vysoká škoda (numericky 1, 2, 3)
- Kritičnost aktiva lze ohodnotit součtem numerických ohodnocení škodních tříd, kterým je aktivum vystaveno
- Potřebná EAL produktů použitých pro ochranu aktiva nechť je funkcí jeho kritičnosti a jeho nejvyšší škodní třídy

Která EAL je vhodná pro náš TOE ? Příklad řešení

- Škodní třídy
  - ✓ C: žádná, nízká, střední, vysoká škoda (numericky 0, 1, 2, 3)
  - ✓ I: nízká, střední, vysoká škoda (numericky 1, 2, 3)
  - ✓ A: nízká, střední, vysoká škoda (numericky 1, 2, 3)
- Příklady kritičností systémů
  - ✓ 2: nízká škodní třída z hlediska integrity a dostupnosti
  - ✓ 3: nízká škodní třída z hlediska integrity, dostupnosti a důvěrnosti
  - ✓ 3: střední škodní třída z hlediska integrity a nízká škodní třída z hlediska dostupnosti
  - ✓ 6: střední škodní třída z hlediska integrity, dostupnosti a důvěrnosti
  - ✓ 9: vysoká škodní třída z hlediska integrity, dostupnosti a důvěrnosti

Která EAL je vhodná pro náš TOE ? Příklad řešení

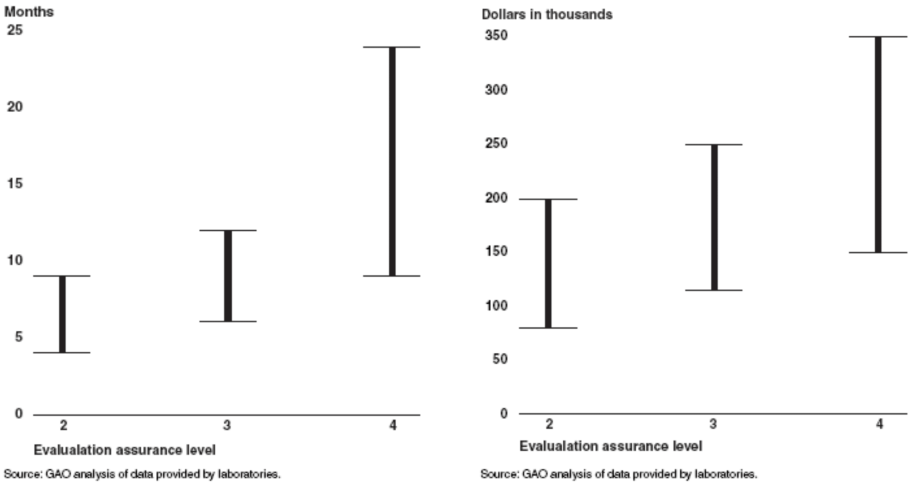
Nejvyšší ze škodních tříd aktiva

	ŠKODNÍ TŘÍDA = 1	ŠKODNÍ TŘÍDA = 2	ŠKODNÍ TŘÍDA = 3
KRITIČNOST = 2	EAL 1		
KRITIČNOST = 3	EAL 2	EAL 3	
KRITIČNOST = 4		EAL 3	EAL 4
KRITIČNOST = 5		EAL 4	EAL 4
KRITIČNOST = 6		EAL 4	EAL 4
KRITIČNOST = 7			EAL 5
KRITIČNOST = 8			EAL 6
KRITIČNOST = 9			EAL 7

Která EAL je vhodná pro náš TOE ? Příklad řešení

- Pro ochranu administrativních dat se škálou škod CIA 0, 1, 1
  tj. nízká škodní třída z hlediska integrity a dostupnosti,
  je vhodná EAL 2
- Pro ochranu web serveru se škálou škod CIA 0, 2, 2,
  tj. střední škodní třída z hlediska integrity a dostupnosti,
  je vhodná EAL 3
- Pro ochranu klíčů PKI se škálou škod CIA 3, 3, 2,
  tj. vysoká škodní třída z hlediska integrity a důvěrnosti a
  střední škodní třída z hlediska dostupnosti,
  je vhodná EAL 6

Co stojí a jak dlouho se řeší hodnocení ranku EAL2-EAL4?



- Zdroj: *US Government Accountability Office, 2006*