Ministerstvo financií
Slovenskej republiky

EFQM
Recognised for excellence
5 star - 2012

Architektúra a hodnotenie

Hodnotenie bezpečnosti informačných systémov

RNDr. Jaroslav Janáček, PhD.
2013

KPMG
cutting through complexity™

Význam kritérií

- definícia požiadaviek na bezpečnosť produktov
  - jednotný spôsob definovania bezpečnostných požiadaviek
  - využitie katalógových požiadaviek
- overovanie naplnenia požiadaviek produktom
  - jednotnosť postupu overenia
- porovnávanie produktov

História kritérií

- TCSEC (Orange Book)
  - 1985, USA
  - 4 skupiny (D, C, B, A)
  - 4 množiny požiadaviek
    - definícia a prostriedky na presadenie bezp. politiky
    - účtovateľnosť aktivít
    - bezpečnostné záruky
    - dokumentácia

História kritérií

- ITSEC
  - 1991, Európa (DE, FR, NL, UK)
  - nepredpisuje funkčné bezp. požiadavky
  - definuje požiadavky na bezp. záruky
  - pre každý produkt vyžaduje **bezpečnostný zámer**
    - bezp. politika, požiadavky na okolie
    - bezp. ciele, bezp. funkcie a mechanizmy
    - deklarovaná sila mechanizmov
    - požiadavky na bezp. záruky
  - 7 úrovní bezp. záruk (E0 až E6)

História kritérií

- Common Criteria (CC)
  - 1993, USA, Kanada, DE, FR, NL, UK
  - 1996 v. 1.0
  - 1998 v. 2.0
    - ISO/IEC 15408-1,2,3:1999
    - v. 2.3 – ISO/IEC 15408-1,2,3:2005
    - v. 3.1 – ISO/IEC 15408-1:2009, 15408-2,3:2008

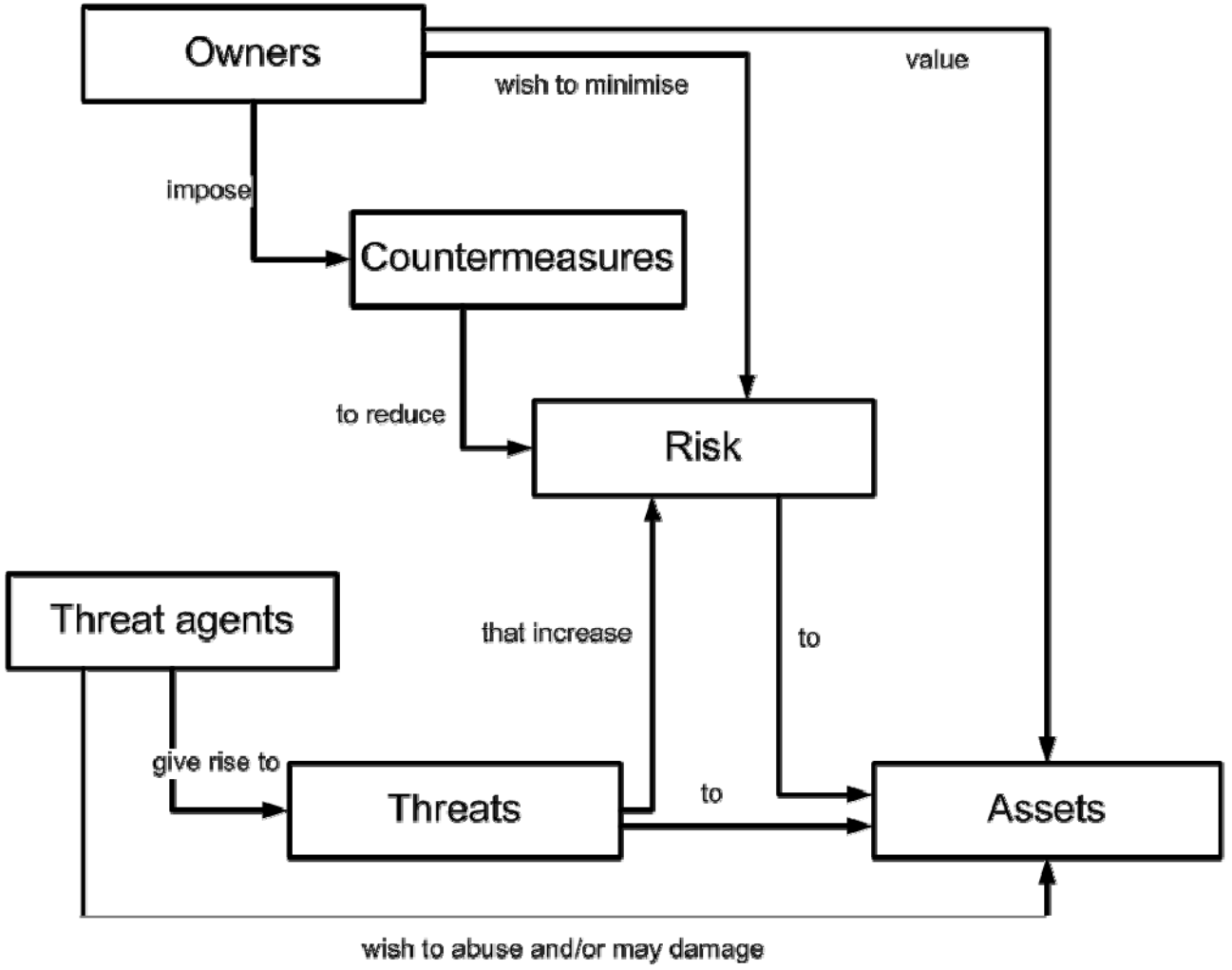
Štruktúra CC

- 3 časti
  - Úvod a všeobecný model
  - Komponenty pre funkčné bezpečnostné požiadavky
  - Komponenty pre požiadavky na bezpečnostné záruky

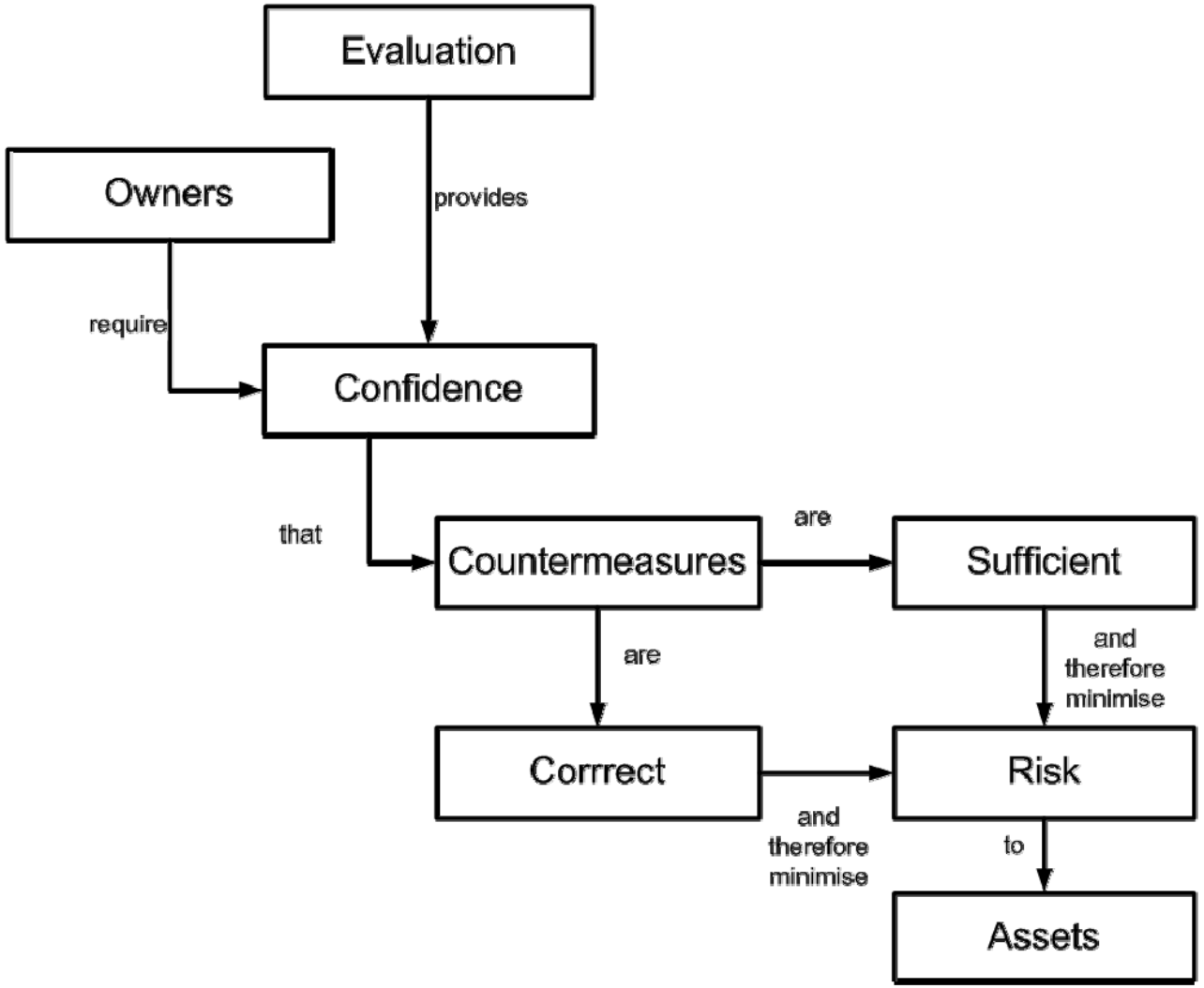
Predmet hodnotenia

- TOE (Target of Evaluation)
  - IT produkt, časť IT produktu, sada IT produktov, ...
  - súčasťou definície TOE môže byť aj predpísaná konfigurácia
  - príklady
    - operačný systém
    - aplikácia
    - kryptografická čipová karta
    - informačný systém ako celok

Základný model



Prínos hodnotenia



Prínos hodnotenia

- dostatočnosť opatrení
  - ak opatrenia robia to, čo deklarujú, tak účinne pôsobia proti hrozbám
- korektnosť opatrení
  - je dostatočný dôvod veriť, že opatrenia robia to, čo deklarujú

Dostatočnosť opatrení

- bezpečnostný zámer (security target, ST) definuje
  - aktíva, hrozby voči nim
  - opatrenia v podobe bezpečnostných cieľov
    - pre TOE
    - pre okolie
  - funkčné bezpečnostné požiadavky pre TOE
    - popísané pomocou komponentov 2. časti CC

Korektnosť opatrení

- bezpečnostný zámer (security target) definuje
  - požiadavky na bezpečnostné záruky (3. časť CC)
    - postupy pri vývoji
    - testovanie
    - súlad jednotlivých reprezentácií TOE v procese vývoja
- korektnosť okolia TOE
  - nutný predpoklad bezpečnosti
  - mimo rozsah hodnotenia podľa CC

Protection profile (PP)

- vzťahuje sa na **typ** TOE
  - napr. operačný systém, kryptografická karta, ...
  - ST sa vzťahuje na konkrétny TOE
- slúži ako základ pre ST
  - ST deklaruje súlad s PP (aj s viacerými)
- hodnotenie PP
  - kompletnosť, konzistentnosť, techická zmysluplnosť a vhodnosť ako základ pre ďalšie PP alebo ST

Hodnotenie podľa CC

- hodnotenie PP
- hodnotenie ST
  - dostatočnosť bezpečnostných cieľov pre TOE a okolie TOE
- hodnotenie TOE
  - dostatočná miera dôvery v korektnosť TOE
  - a teda napokon v bezpečnosť prevádzkovaného TOE za predpokladu korektného okolia

Štruktúra ST

- úvod
  - identifikácia, prehľad a popis TOE
- deklarácia súladu (s CC, PP)
- definícia bezpečnostného problému
  - hrozby
  - organizačné bezp. politiky
  - predpoklady o okolí

Štruktúra ST (2)

- bezpečnostné ciele (security objectives)
  - pre TOE
  - pre okolie
  - zdôvodnenie
    - každý cieľ je zdôvodnený hrozbou, politikou alebo predpokladom
    - všetky hrozby, politiky a predpoklady sú dostatočne zohľadnené bezpečnostnými cieľmi

Štruktúra ST (3)

- definícia rozšírených komponentov
- bezpečnostné požiadavky
  - funkčné bezpečnostné požiadavky
  - požiadavky na bezpečnostné záruky
  - zdôvodnenie
    - pokrytie medzi cieľmi a funkčnými požiadavkami
    - zdôvodnenie požiadaviek na záruky
- sumárna špecifikácia TOE

Štruktúra PP

- úvod
- deklarácia súladu
- definícia bezpečnostného problému
  - hrozby, politiky, predpoklady o okolí
- bezpečnostné ciele
  - pre TOE, okolie, zdôvodnenie
- definícia rozšírených komponentov
- bezpečnostné požiadavky
  - funkčné, záruky, zdôvodnenie

Štruktúra bezpečnostných požiadaviek podľa CC

- členenie
  - trieda (class)
  - rodina (family)
  - komponent
    - najmenší celok, ktorý môže byť použitý v PP/ST
    - môžu byť hierarchické
  - element

Štruktúra bezpečnostných požiadaviek podľa CC

- operácie na prispôsobenie komponentu
  - iterácia
    - opakované použitie komponentu
  - priradenie (assignment)
    - doplnenie parametrov
  - výber (selection)
    - výber z možných parametrov
  - zjemnenie (refinement)
    - spresnenie

Funkčné bezpečnostné požiadavky

- každá rodina požiadaviek
  - špecifikuje svoj bezpečnostný cieľ
  - hierarchiu komponentov
  - požiadavky na manažment parametrov
  - auditovateľné udalosti
- komponent
  - okrem elementov špecifikuje závislosti na iných komponentoch

Funkčné bezpečnostné požiadavky

- FAU – Bezpečnostný audit (Security audit)
  - generovanie, filtrovanie, ukladanie, prezeranie, analýza auditných záznamov (logov) o bezpečnostne relevantných aktivitách
  - automatická reakcia na výskyt určených bezpečnostne relevantných udalostí

Funkčné bezpečnostné požiadavky

- FCO – Komunikácia (Communication)
  - zabezpečenie spoľahlivej identifikácie odosielateľa a prijímateľa informácie
  - zabezpečenie nepopierateľnosti odoslania / prijatia informácie

Funkčné bezpečnostné požiadavky

- FCS – Kryptografická podpora (Cryptographic support)
  - manažment kryptografických kľúčov
  - vykonávanie kryptografických operácií

Funkčné bezpečnostné požiadavky

- FDP – Ochrana používateľských údajov (User data protection)
  - politiky bezp. funkcií
    - politika riadenia prístupu
    - politika riadenia toku informácie
  - spôsob ochrany údajov
    - riadenie prístupu, riadenie toku informácie
    - vnútorné prenosy, ochrana zvyškovej informácie, ochrana integrity uložených údajov
  - offline ukladanie, import, export
  - komunikácia medzi dôveryhodnými systémami

Funkčné bezpečnostné požiadavky

- FIA – Identifikácia a autentizácia (Identification and authentication)
  - požiadavky na identifikáciu a autentizáciu používateľov
  - špecifikácia bezp. atribútov používateľov
  - požiadavky na väzbu atribútov používateľa a procesov
  - požiadavky na reakciu na chyby autentifikácie
  - požiadavky na zaistenie kvality hesiel

Funkčné bezpečnostné požiadavky

- FMT – Správa bezpečnosti (Security management)
  - správa bezpečnostných atribútov, údajov a funkcií
  - expirácia bezp. atribútov
  - definícia bezp. rol a ich vzťahov

Funkčné bezpečnostné požiadavky

- FPR – Ochrana súkromia (Privacy)
  - požiadavky na ochranu súkromia používateľov
  - anonymita, pseudoanonymita
  - nespojiteľnosť aktivít
  - nesledovateľnosť aktivít

Funkčné bezpečnostné požiadavky

- FPT – Ochrana bezp. funkcií (Protection of the TSF)
  - ochrana implementácie
  - ochrana bezp. údajov
  - externé entity využívané bezp. funkciami
  - zaistenie bezpečnosti aj v chybových stavoch a bezpečná obnova činnosti
  - fyzická ochrana
  - testovanie

Funkčné bezpečnostné požiadavky

- FRU – Využívanie zdrojov (Resource utilisation)
  - odolnosť voči zlyhaniam vybraných zdrojov
  - prideľovanie zdrojov, priority
  - obmedzovania využívania zdrojov

Funkčné bezpečnostné požiadavky

- FTA – Prístup k systému (Access)
  - obmedzenie prístupu používateľov k systému
  - uzamykanie a ukončovanie session
  - zobrazovanie histórie prístupu

Funkčné bezpečnostné požiadavky

- FTP – Dôveryhodná cesta/kanál (Trusted path/channel)
  - požiadavky na dôveryhodné komunikačné kanály medzi systémami
  - požiadavky na dôveryhodnú komunikačnú cestu medzi systémom a používateľom
  - dôveryhodná
    - zaistená identita oboch koncov
    - komunikácia chránená pred nedôveryhodnými aplikáciami

Požiadavky na bezp. záruky

- elementy komponentu sú členené na
  - požiadavky na činnosti pri vývoji
  - obsah a požiadavky na prezentáciu „dôkazov“
  - požiadavky na činnosť hodnotiteľa

Požiadavky na bezp. záruky

- ADV – Vývoj (Development)
  - popis návrhu a implementácie funkčných bezp. požiadaviek
  - bezp. architektúra pre separáciu domén, neobíditeľnosť a vlastnú ochranu
  - model bezp. politiky a preukázanie jej súladu s funkčnou špecifikáciou
  - vnútorná štruktúra bezp. funkcií

Požiadavky na bezp. záruky

- AGD – Dokumentácia (Guidance documents)
  - požiadavky na dokumentáciu TOE
    - prípravnú
      - ako bezpečne nainštalovať a nakonfigurovať TOE
    - prevádzkovú
      - ako bezpečne prevádzkovať TOE
  - pre rôzne roly
      - používateľskú, administrátorskú, vývojársku, ...

Požiadavky na bezp. záruky

- ALC – Pdpora životného cyklu (Life cycle support)
  - popis životného cyklu
  - manažment konfigurácií
  - bezpečnosť vývojového prostredia
  - popis vývojových nástrojov a postupov
  - bezpečná distribúcia TOE
  - odhaľovanie a odstraňovanie chýb

Požiadavky na bezp. záruky

- ATE – Testy (Tests)
  - pokrytie testami
  - hĺbka testovania
  - funkčné testovanie
  - nezávislé testovanie

Požiadavky na bezp. záruky

- AVA – Posúdenie zraniteľností (Vulnerability assessment)
  - požiadavky na hľadanie zraniteľností TOE
    - penetračné testovanie
    - analýza návrhu s cieľom odhaliť potenciálne zraniteľnosti
    - analýza kódu s cieľom odhaliť potenciálne zraniteľnosti

Požiadavky na bezp. záruky

- ACO – Skladanie (Composition)
  - požiadavky na skladanie TOE z menších, hodnotených TOE s cieľom zaistiť bezpečné fungovanie zloženého TOE
- ASE – Hodnotenie ST
- APE – Hodnotenie PP

Úrovne hdnotenia – EAL

- jednotlivé úrovne sú definované množinou požiadaviek na bezpečnostné záruky
  - nanajvýš jeden komponent z rodiny
    - vyššie úrovne požadujú silnejšie komponenty
  - všetky komponenty potrebné na uspokojenie závislostí

EAL1 – funkčne testovaný

- ciele
  - základná dôvera v korektné správanie
  - hrozby nie sú považované za vážne
  - bez potreby spolupráce vývojára pri hodnotení
  - konzistencia fungovania TOE s dokumentáciou
- záruky
  - aspoň čiastočný ST a analýza funkčných bezp. požiadaviek použitím funkčnej špecifikácie, špecifikácie rozhraní a dokumentácie
  - nezávislé funkčné a penetračné testovanie proti známym zraniteľnostiam
  - jednoznačná identifikácia TOE a súvisiacich dokumentov

EAL2 – štrukturálne testovaný

- ciele
  - vyžaduje spoluprácu s vývojárom v podobe dodania návrhu TOE a výsledkov testov
  - nižšia až stredná úroveň nezávislého potvrdenia bezpečnosti bez prístupu ku kompletnej vývojovej dokumentácii

EAL2 – štrukturálne testovaný

- záruky
  - plný ST, analýza funkčných bezp. požiadaviek aj s použitím základného popisu architektúry
  - špecifikácia a výsledky testovania vývojárom oproti funkčnej špecifikácii
  - nezávislé potvrdenie vybraných testov
  - analýza zraniteľností použitím funkčnej špecifikácie, návrhu a bezp. architektúry, preukázanie odolnosti voči útočníkom vo základným útočným potenciálom
  - manažment konfigurácie a bezpečná distribúcia

EAL3 – metodicky testovaný a kontrolovaný

- ciele
  - maximálne záruky pri zohľadnení bezpečnostných aspektov pri návrhu bez potreby podstatnej úpravy vývojových postupov
  - stredná úroveň nezávislého potvrdenia bezpečnosti vrátane dôkladného preskúmania TOE a jeho vývoja bez potreby jeho podstatného prerábania

EAL3 – metodicky testovaný a kontrolovaný

- záruky
  - vyššie požiadavky na popis návrhu použitý pri analýze bezp. funkčných požiadaviek
  - testovanie vývojárom aj s využitím návrhu
  - vyššie požiadavky na manažment konfigurácií
  - požiadavky na kontrolované vývojové prostredie

EAL4 – metodicky navrhnutý, testovaný a revidovaný

- ciele
  - maximálne záruky pri zohľadnení bezpečnostných aspektov použitím dobrých vývojových postupov bez potreby podstatných špeciálnych znalostí a schopností
  - stredná až vysoká úroveň nezávislého potvrdenia bezpečnosti s ochotou znášať vyššie náklady spojené s bezpečným vývojom

EAL4 – metodicky navrhnutý, testovaný a revidovaný

- záruky
  - pri analýze funkčných bez. požiadaviek sa vychádza aj z úplnej špecifikácie rozhraní, základného modulárneho návrhu a častí implementácie
  - analýza zraniteľností aj s použitím implementácie, preukázanie odolnosti proti útočníkovi s rozšíreným základným útočným potenciálom
  - ďalšie požiadavky na manažment konfigurácií vrátane automatizácie

EAL5 – semiformálne navrhnutý a testovaný

- ciele
  - maximálne záruky pri zohľadnení bezpečnostných aspektov použitím dôsledných vývojových postupov vrátane primeraného využitia špeciálnych techník pre vývoj bezpečných systémov
  - vysoká úroveň nezávislého potvrdenia bezpečnosti s cieleným vývojom, dôsledné postupy bez prehnane vysokých nákladov na špeciálne postupy

EAL5 – semiformálne navrhnutý a testovaný

- záruky
  - vyžaduje sa modulárny návrh
  - vyžaduje sa nezávislá analýza zraniteľností a odolnosť voči útočníkovi so stredným útočným potenciálom
  - vyžaduje sa rozsiahlejší manažment konfigurácie

EAL6 – semiformálne overený návrh a testovaný

- ciele
  - vysoké záruky z použitia špeciálnych postupov pre vývoj bezpečných systémov s cieľom vytvoriť prémiový produkt pre ochranu hodnotných aktív proti významným rizikám
  - určené pre vysoko rizikové prostredie, kde hodnota aktív ospravedlňuje vysoké náklady na bezpečnosť

EAL6 – semiformálne overený návrh a testovaný

- záruky
  - vyžaduje sa formálny model vybraných bezpečnostných politík, semiformálna prezentácia funkčnej špecifikácie a návrhu, a modulárny, vrstvový s jednoduchý návrh
  - nezávislá analýza zraniteľností a odolnosť voči útočníkovi s vysokým útočným potenciálom
  - vyžaduje sa štruktúrovaný vývojový proces, plná automatizácia manažmentu konfigurácií

EAL7 – formálne overený návrh a testovaný

- ciele
  - bezpečnostné produkty pre extrémne rizikové prostredie
- záruky
  - pri analýze funkčných bezp. požiadaviek sa použije aj štrukturovaná reprezentácia implementácie
  - testuje sa celá reprezentácia implementácie, nezávisle sa musia potvrdiť všetky výsledky testov

Prínosy EAL

- EAL2 oproti EAL1
  - testovanie pri vývoji, analýza zraniteľností, nezávislé testovanie s viac detailami
- EAL3 oproti EAL2
  - vyššie pokrytie testami, základná bezpečnosť vývojového prostredia
- EAL4 oproti EAL3
  - podrobnejší popis návrhu, reprezentácia implementácie, vyššie požiadavky na vývojové prostredie

Prínosy EAL

- EAL5 oproti EAL4
  - semiformálny návrh, štrukturovanejšia architektúra
- EAL6 oproti EAL5
  - podrobnejšia analýza, štrukturovaná reprezentácia implementácie, štrukturovanejšia architektúra (vrstvy, ...), podrobnejšia nezávislá analýzy zraniteľností, lepší manažment konfigurácie a prostredie
- EAL7 oproti EAL6
  - formálne reprezentácie a formálna korešpondencia, podrobnejšie testovanie

Využitie CC v praxi

- tvorba ST a PP je náročný proces
- hodnotenie je ešte náročnejší proces
  - niekedy to môže byť príliš v porovnaní s významom a cenou informačného systému
- filozofia CC je však použiteľná
  - definovať problém
  - navrhnúť a zdôvodniť riešenie
  - dobre definovať predpoklady a požiadavky na okolie

Využitie CC v praxi

- informácia „produkt ohodnotený (alebo aj ceritfikovaný) na EALx“
  - nehovorí veľa bez príslušného ST
  - neznamená veľa bez dodržania predpokladov

Register PP a certifikovaných produktov

- register na portáli http://www.commoncriteriaportal.org/
  - vyhodnotené PP
  - register certifikovaných produktov

Otázky?

Ďakujem za pozornosť.