Aplikační bezpečnost

Ing. Vladimír Lazecký
vladimir.lazecky@viavis.cz

VIAVIS střežíme podstatné

Common Criteria (ISO/IEC 15408) – zdroj informací

https://www.commoncriteriaportal.org/

Zdroj informací – zastaralé, ale stejné principy

The Common Criteria

Published: August 10, 2006 | Last revised: July 05, 2013

Author(s): Nancy Mead

Maturity Levels and Audience Indicators: L4 / L

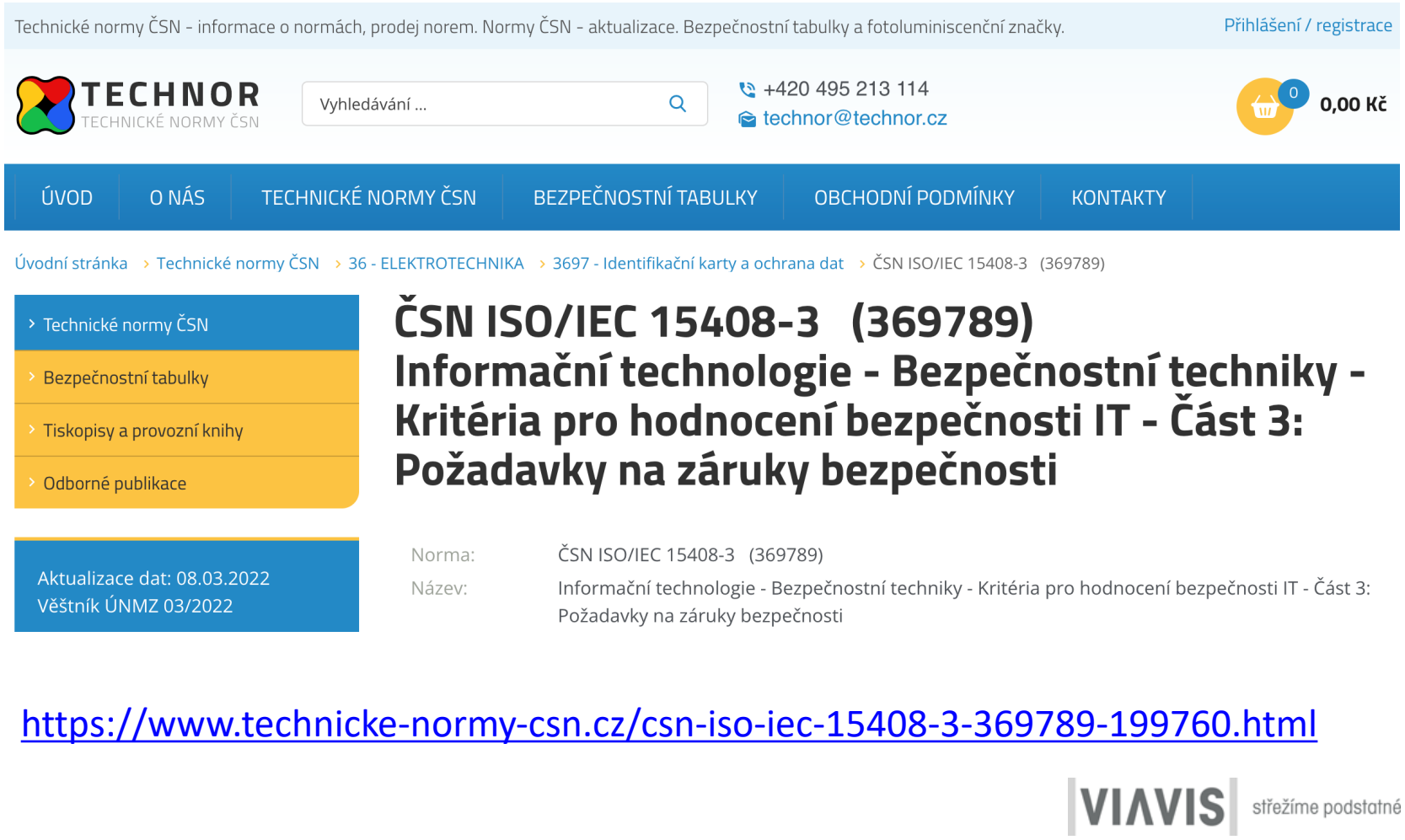
SDLC Life Cycles: Requirements

Abstract

The Common Criteria enable an objective evaluation to validate that a particular product or system satisfies a defined set of security requirements. Although the focus of the Common Criteria is evaluation, it presents a standard that should be of interest

https://www.cisa.gov/uscert/bsi/articles/best-practices/requirements-engineering/the-common-criteria

Zdroje informací ČR, paradoxy normativů…



https://www.technicke-normy-csn.cz/csn-iso-iec-15408-3-369789-199760.html

Cíle CC

- Ověření/validace že:
  - Systém splňuje **definované** bezpečnostní požadavky
- CC jsou více zaměřeny na ověření/validaci
- CC jsou méně orientovány na způsob realizace bezpečnostních požadavků
- Inspirace pro způsob řízení a vedení vývoje

CC – ISO/IEC 15408

- Tvoří rámec, ve kterém:
  - Uživatelé specifikují požadavky
  - Výrobci tyto požadavky implementují a prohlašují o výrobku, že je splňuje
  - Testováním je vyhodnoceno, že produkt je takový, za jaký je prohlášen
- **Common Criteria poskytují záruku, že proces specifikace, implementace a evaluace ICT produktu byl proveden přesným a standardním postupem.**

CC – ISO/IEC 15408

- **ISO/IEC 15408 1-3**
- Česká verze
  - ČSN ISO/IEC15408-1 – Úvod a všeobecný model
  - ČSN ISO/IEC15408-2 – Bezpečnostní funkční požadavky
  - ČSN ISO/IEC15408-3 – Požadavky na záruky bezpečnosti

Základní pojmy CC

- **Target of Evaluation TOE** – předmět hodnocení
  - IT produkt, systém nebo jejich část podléhající hodnocení
  - Cílem hodnocení TOE je ověření, zda jsou splněny všechny požadavky, specifikace bezpečnosti
  - Prokázání shody s implementovaným vzorem

Základní pojmy – Protection Profile

- PP - bezpečnostní profil:
  - Definice implementačně **nezávislé sady požadavků a cílů pro třídu produktů** nebo systémů, které odpovídají obdobným uživatelským potřebám informační bezpečnosti s ohledem na hrozby existující ve specifickém prostředí
  - PP byly vyvinuty pro různé produkty - databáze, firewally, čipové karty…

Pro inspiraci – Protection Profile

NIAP »» Protection Profiles »» Approved PPs »» Details

U.S. Government Approved Protection Profile - Protection Profile for Certification Authorities Version 2.1

Short Name: pp_ca_v2.1

Technology Type: Certificate Authority

CC Version: 3.1

Date: 2017.12.01

Transition End Date: 2018.06.01

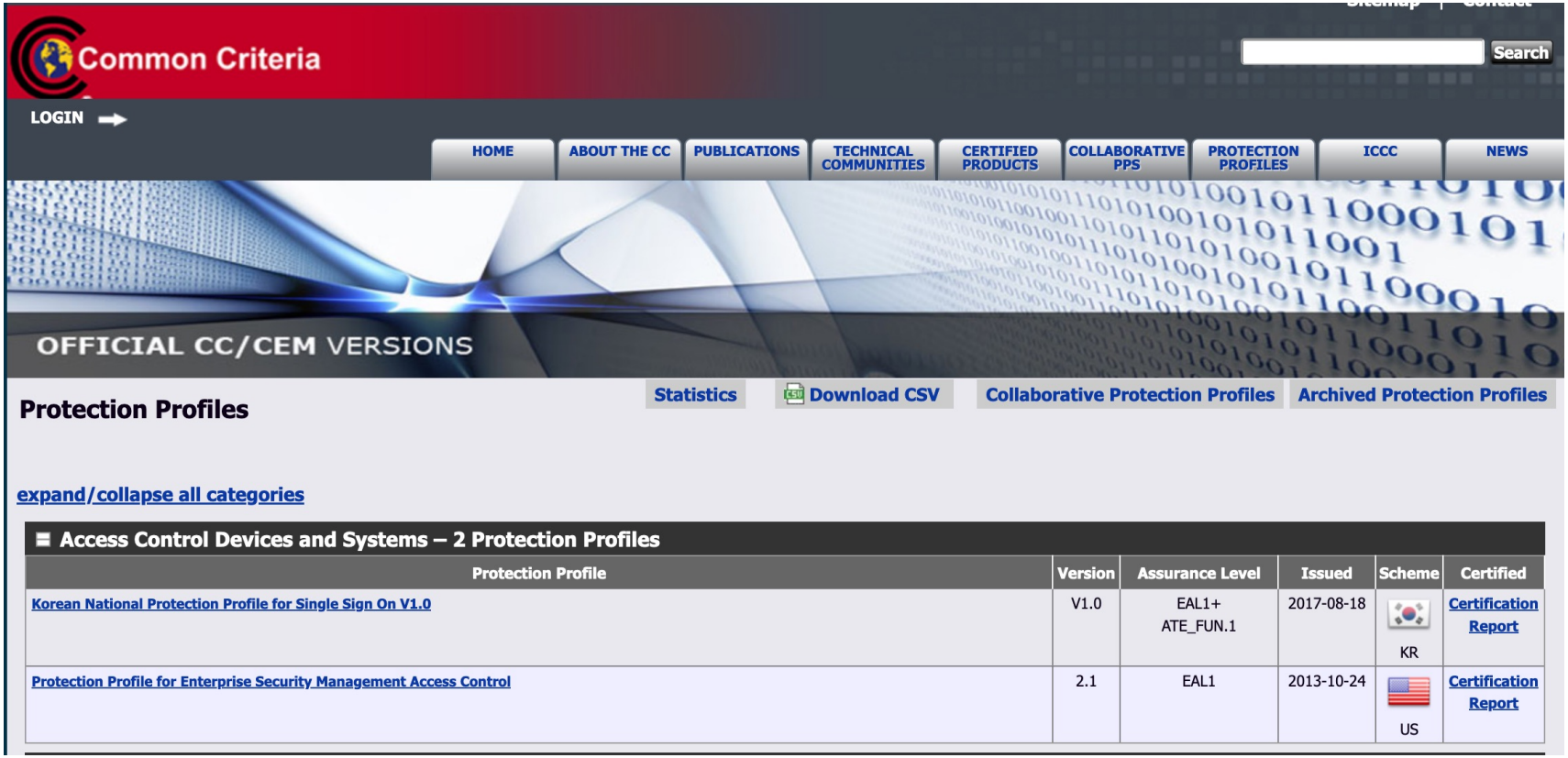
Preceded By: pp_ca_v2.0

Conformance Claim: None

Protection Profile

https://www.niap-ccevs.org/profile/Info.cfm?PPID=420&id=420

Pro inspiraci – Protection Profile



https://www.commoncriteriaportal.org/pps/

VIAVIS střežíme podstatné

Pro inspiraci – Protection Profile

Federal Office
for Information Security

Fingerprint Spoof Detection Protection Profile

based on Organisational Security Policies

FSDPP_OSP

v1.7

https://www.commoncriteriaportal.org/files/ppfiles/pp0062b_pdf.pdf

VIAVIS střežíme podstatné

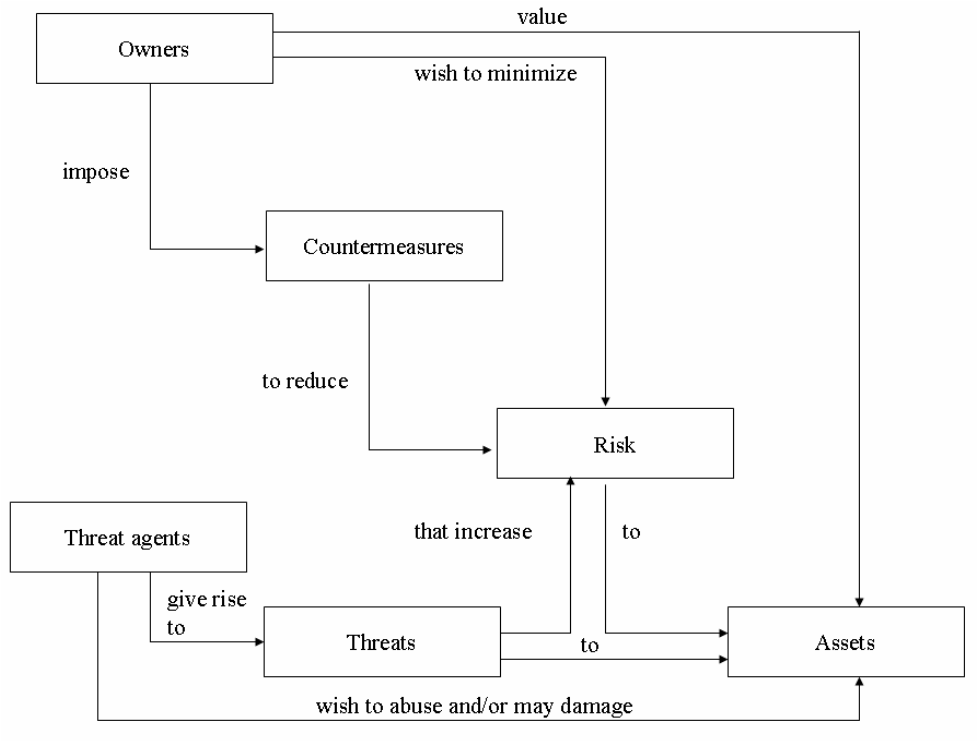
Základní pojmy – Security Target

- ST - Security Target – bezpečnostní cíl:
  - Specifikace a požadavky na informační bezpečnost pro konkrétní systém nebo produkt
  - Nad rámec PP obsahuje popis bezpečnostních funkcí TOE s vysvětlením požadavků na záruky
  - Je používán jako základ pro hodnocení TOE.

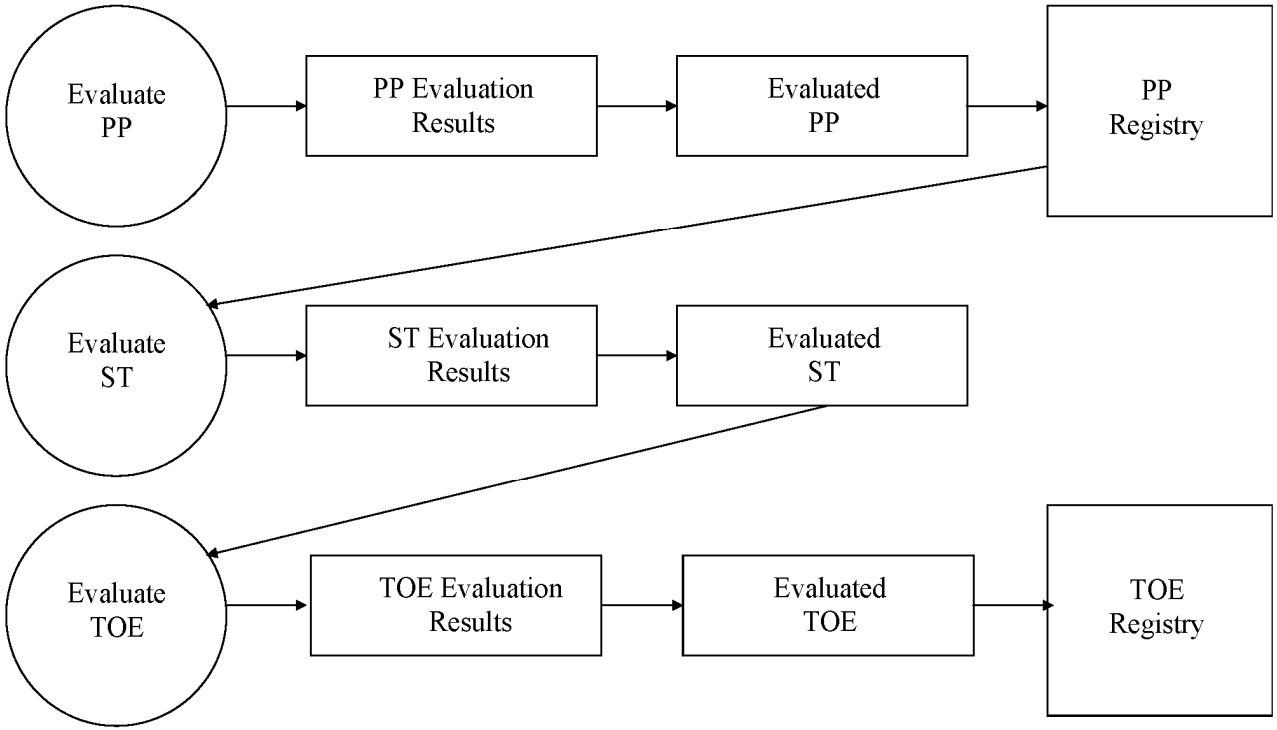
Základní pojmy - hodnocení

- **Hodnocení**:
  - Etalon hodnocení je ST (Security Target)
  - Vstup je ST, množina důkazů ohledně TOE a vlastní TOE
  - Výstup je potvrzení, že ST jsou naplněny prostřednictvím TOE
  - Hodnocení je sada dokumentů
- **Provoz** – může vyvolat požadavek na opětovné hodnocení (unikátní prostředí)

Základní bezpečnostní koncept – zdroj CC



Principy hodnocení – zdroj CC



Security Target

- ST – dohoda mezi uživateli, vývojáři a evaluačními autoritami – jakou bezpečnost TOE nabízí, rozsah hodnocení..

- Struktura dokumentu ST
  - Úvod
  - Popis TOE
  - Bezpečnostní prostředí TOE
  - Bezpečnostní cíle
  - Požadavky na bezpečnost IT
  - Požadavky uplatňované v PP
  - Shrnutí specifikací TOE
  - Zdůvodnění

Základní pojmy TSP, TSF

- **TSP (TOE Security Policy) –** bezpečnostní politika hodnoceného předmětu:
  - Pravidla pro správu, ochranu a distribuci aktiv v rámci TOE
- **TSF (TOE Security Functions) –** bezpečnostní funkcionalita hodnoceného předmětu:
  - Všechny části (HW a SW) TOE, jejichž činnosti se vztahují k prosazení pravidel TSP

ISO/IEC 15408 – 1 Část I. – Úvod a obecný model - určení

- ✓ Uživatelé – základní informace a reference
- ✓ Vývojáři - základní informace a reference pro vývoj požadavků a formulace bezpečnostních specifikací pro TOE
- ✓ Hodnotitelé - základní informace a reference. Popis struktury pro PP a ST

ISO/IEC 15408 – 1 Část II. – Požadavky a bezpečnostní funkce

- **Uživatelé** – návod a reference pro formulaci vyjádření požadavků na bezpečnostní funkce

- **Vývojáři** – reference pro interpretaci vyjádření funkčních požadavků a formulaci funkčních specifikací TOE

- **Hodnotitelé** – závazné vyjádření evaluačních kritérií pro určení, zda TOE účinně vyhovuje požadovaným bezpečnostním funkcím

ISO/IEC 15408 – 1 Část III. – Požadavky na bezpečnostní záruky

- **Uživatelé** - návod k určení požadovaných úrovní bezpečnostních záruk

- **Vývojáři** – reference pro interpretaci vyjádření požadavků na záruky a určení přístupu TOE k bezpečnostním zárukám

- **Hodnotitelé** - závazné vyjádření evaluačních kritérií pro určení bezpečnostních záruk

Bezpečnostní rámec

- Zahrnuje:
  - **Bezpečnostní prostředí** – zákony, bezpečnostní politika, hrozby v prostředí
  - **Bezpečnostní plány** – záměry odolat identifikovaným hrozbám a/nebo naplnit předpoklady a záměry bezpečnostní politiky
  - **Bezpečnostní požadavky TOE** – rozpracování bezpečnostních plánů do sady technických bezpečnostních požadavků na bezpečnostní funkce a záruky
  - **Bezpečnostní specifikace TOE** – definice aktuálních nebo navrhnutých implementací TOE
  - **Implementace TOE** – realizace TOE v souladu s jeho specifikací

11 tříd požadavků na bezpečnostní funkce

- **FAU (Security Audit)** – bezpečnostní audit
- **FCO (Communication)** - komunikace
- **FCS (Cryptographic Support)** - kryptografická podpora
- **FDP (User Data Protection)** - ochrana dat uživatelů
- **FIA (Identification and Authentication)** - identifikace a autentizace,
- **FMT (Security Management)** - management bezpečnosti
- **FPR (Privacy)** - soukromí
- **FPT (Protection of TSF)** - ochrana TSF
- **FRU (Resource Utilisation)** - použití zdrojů
- **FTA (TOE Access)** - přístup k TOE,
- **FTP (Trusted Path/Channel)** - bezpečný komunikační kanál

Katalog požadavků na bezpečnostní záruky

Třída obecných požadavků na bezpečnostní záruky

- Třída ACM (Configuration Management) - správa konfigurace (udržování integrity bezpečnostních parametrů TOE)
- Třída ADO (Delivery and Operation) - dodávka, instalace a provoz
- Třída ADV (Development) - vývoj TOE
- Třída AGD (Guidance Documents) - obsah bezpečnostní dokumentace
- Třída ALC (Life Cycle Support) - podpora životního cyklu TOE
- Třída ATE (Tests) - rozsah, hloubka a nezávislost testů TOE
- Třída AVA (Vulnerability Assessment) - zranitelnost TOE (analýza skrytých kanálů a jiných zranitelných míst)

Katalog požadavků na bezpečnostní záruky

- Třída uchování záruk:
  - Třída AMA (Maintenance of Assurance) - údržba záruk (zachování záruk po možných změnách v provozním prostředí)

Katalog požadavků na bezpečnostní záruky

- Kritéria pro hodnocení PP a ST:
  - Třída APE (Protection Profile Evaluation) - hodnocení profilu bezpečnosti (PP) prokazuje jeho vhodnost a kvalitu
  - Třída ASE (Security Target Evaluation) - hodnocení cílů bezpečnosti (ST) vzhledem ke všem požadavkům spojeným s tímto cílem

Katalog požadavků na bezpečnostní záruky

- Speciální účelová sada – úrovně hodnocení záruk – množiny komponent z rodin požadavků na bezpečnostní záruky:

  - Rovnoměrné uspořádání požadavků směřující k vyváženému pohledu na míru důvěry v korektnost TOE

  - Úrovně záruk jsou určeny k zajištění pětné kompatibility se „zdrojovými“ kritérii

  - Vnitřní konzistence účelových sad bezpečnostních záruk (assurance packages)

Úrovně záruk EAL1 – EAL7

EAL1: **Funkčně testováno -** poskytuje jistou míru důvěry na základě funkční specifikace, vymezení rozhraní a zpracování dokumentace

EAL2: Strukturovaně testováno - nezávislé testování. Vývoj rozšířen o neformální popis architektury a popis ošetření běžných útoků

EAL3: Metodicky testováno a kontrolováno - maximální záruky na základě osvědčeného svědomitého přístupu k vývojovému procesu (bez navýšení náročnosti)

EAL4: Metodicky navrženo, testováno a kontrolováno - vyžaduje velmi kvalitní vývojové praktiky, které ale nevyžadují speciální znalosti a zdroje. Detailní popis návrhu s doložením odolnosti proti útoků s omezenými zdroji. **EAL4 je nejvyšší úrovní na komerční únosnosti**.

Úrovně záruk EAL 1 – EAL 7

EAL5: Poloformálně navrženo a testováno – vyžaduje zapojení specializovaných metod vývoje (formální model). Vyžaduje strukturovaný návrh a základní analýzu skrytých kanálů

EAL6: Poloformálně ověřený a testovaný návrh - vychází z modulárního vrstveného návrhu. Vývoj v max. řízeném prostředí. Vysoká odolnost proti útokům

EAL7: Formálně ověřený a testovaný návrh - vychází z plně formálního návrhu. Vývoj vyžaduje nesmírné náklady - prakticky nepoužitelné

Tolik teorie, pojďme si to zkusit…

- Navrhněme:
  - TOE – Target of Evaluation
  - SP – Security Profile
- Vše co možná nejvíce prakticky…

TOE - Target of Evaluation

Examples of TOEs include:

- A software application;
- An operating system;
- A software application in combination with an operating system;
- A software application in combination with an operating system and a workstation;
- An operating system in combination with a workstation;
- A smart card integrated circuit;
- The cryptographic co-processor of a smart card integrated circuit;
- A Local Area Network including all terminals, servers, network equipment and software;
- A database application excluding the remote client software normally associated with that database application;

Target of Evaluation

- POZOR – nutná definice z pohledů:
  - Uživatel
  - Vývojář
  - Hodnotitel

Security Target – jak na něj ale prakticky

- Analýza rizik pomůže
  - Aktiva a jejich hodnota
  - Zranitelnost
  - Hrozba a její dopad
  - Míra rizika
  - Protiopatření – definice požadavku

Máte nějaké dotazy?

Děkuji za pozornost

Ing. Vladimír Lazecký