Kritéria hodnocení bezpečnosti informačních systémů

Z FITwiki

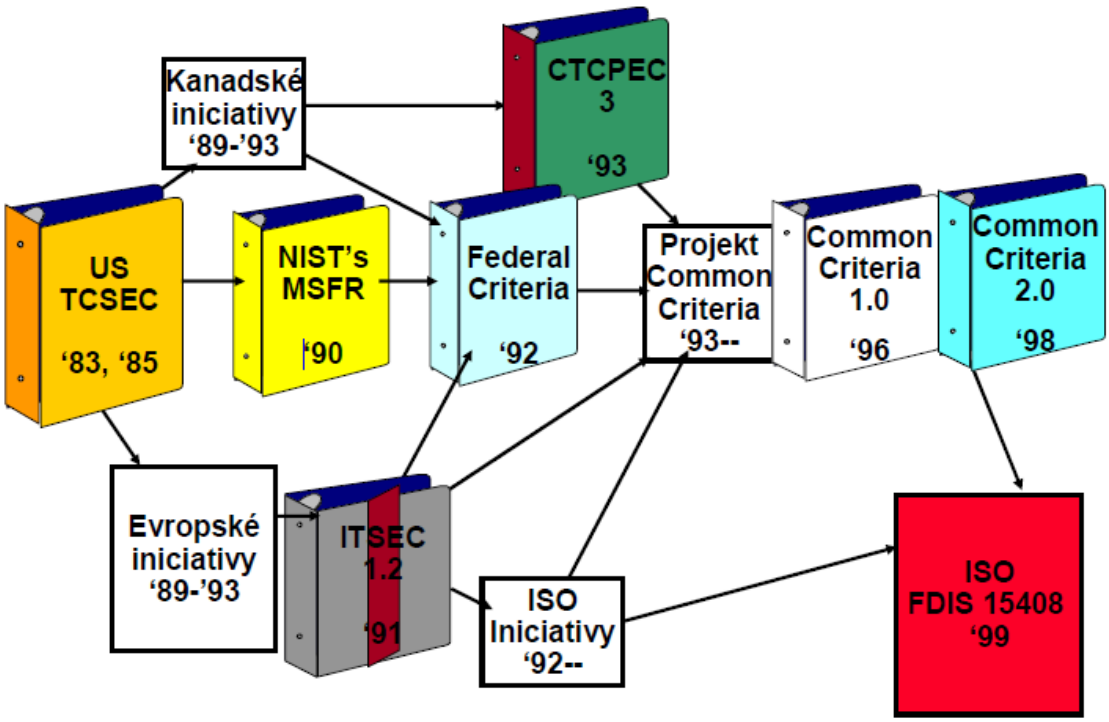
Kritéria se nezabývají opatřeními (logické i fyzické), metodologií hodnocení, dohodami o uznávání, akreditací a kryptografickými algoritmy.

Funkčnost (functionality)
: co je implementováno

Zaručitelnost (assurance)
: míra důvěry, že je to implemenotváno správně

Obsah

Historie



Orange Book (TCSEC)

- první kniha z Rainbow series (série knih o bezpečnosti od Department of Defense USA)

TCSEC
: Trusted Computer System Evaluation Criteria

Úrovně TCSEC

- **D** -- *minimální ochrana*
- **C1** -- *nepovinná ochrana*
  - identifikace, autentizace, nepovinné řízení přístupu
- **C2** -- *ochrana řízeného přístupu*
  - opětné použití a audit
- **B1** -- *víceúrovňová ochrana*
  - povinné řízení přístupu pro některé objekty a subjekty
  - neformální model bezpečnostní politiky
- **B2** -- *strukturovaná ochrana*
  - povinné řízení přístupu pro všechny objekty a subjekty
  - formální model bezpečnostní politiky
  - bezpečná cesta přihlášení
  - princip minimálních privilegií
  - analýza paměťových skrytých kanálů
  - správa konfigurace
- **B3** -- *bezpečnostní domény*
  - analýza všech skrytých kanálů
  - mechanismus validace referencí (ref. monitor)
  - omezení na vytváření kódu
  - požadavky na dokumentaci a testování
- **A1** -- *verifikovaný návrh*
  - formální analýza a verifikace
  - důvěryhodná distribuce

Úrovně TCSEC v praxi

- `C1`, `C2` -- mírně vylepšené současné operační systémy, aplikace nepoznají
- `B1` -- operační systémy se musejí pozměnit více (MAC), některé aplikace vyžadují změny (málo)
- `B2` -- OS jsou změněny zásadně, aplikace nefungují
- `B3` -- systémy, které nezvládly A1 (stejná funkčnost, ale formální návrh)
- `A1` -- systémy navržené od základu, netradiční metody

Oblasti TCSEC

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

Nedostatky TCSEC

- Chybí integrita dat
- Nezná počítačovou síť
- **Nerozlišuje funkčnost a zaručitelnost** (funkčnost - co je implementováno, zaručitelnost - míra důvěry, že je to implementováno správně)
- Různé úrovně abstrakce v dokumentu

Index rizika
se používá k vyjádření stupně bezpečnosti systému. Podle něj se určuje požadovaná úroveň dle TCSEC (stupnice pro otevřené a uzavřené prostředí).
Index rizika $I = R_{max} - R_{min}$

R_{max} je citlivost dat (neklasifikovaná až přísně tajná)
R_{min} je prověření uživatele (neprověřený až prověřen pro přísně tajné).

ITSEC / ITSEM

- jsou evropská kritéria, která vznikla spojením národních kriterií jako alternativa k TCSEC.
- Rozlišuje produkty a systémy
- Rozlišuje funkčnost a zaručitelnost

ITSEC = IT Security Evaluation Criteria (1991)
ITSEM = IT Security Evaluation Manual (1993)

Úrovně funkčnosti ITSEC
F-C1 až F-B3 (odpovídají TCSEC)

Úrovně zaručitelnosti

- **E1** – jsou definovány bezpečnostní cíle, má neformální popis architektury
- **E2** – neformální popis návrhu, kontrola nad konfigurací, distribuční kontrola
- **E3** – korespondence mezi kódem a bezpečnostním cílem
- **E4** – formální model bezpečnostní politiky, strukturovaný přístup k designu, analýza zranitelností vyplývajících z návrhu
- **E5** – korespondence mezi návrhem a kódem, analýza zranitelnosti zdrojového kódu
- **E6** – formální metody architektury a mapování návrhu na bezpečnostní politiku

Třídy funkčnosti

- **F-IN** - integrita
- **F-AV** - dostupnost
- **F-DI** - integrita přenosu dat
- **F-DC** - důvěrnost přenosu dat

Síla mechanismů ITSEC
: pouze vágní v praxi nepoužitelná definice

- **základní** - proti náhodným poruchám
- **střední** - proti útočníkovi s omezenými prostředky
- **vysoká** - prosti útočníkům s vysokými prostředky

Síla mechanismů ITSEM
: přesnější specifikace

Bere v úvahu:

- *Znalosti* - jak moc útočník zná produkt (začátečník, zkušený, expert)
- *Prostředky*
  - Čas - čas a provedení (minuty, dny, měsíce)
  - Vybavení - (bez vybavení, běžné vybavení, speciální vybavení)
- *Příležitost* - neovlivněno útočníkem (komplot, šance, možnost detekce)

Common Criteria

: jsou standardizovaná (ISO/EIC) kritéria hodnocení bezpečnosti systémů. Existuje dohoda vzájemného uznávání a státy mají národní schémata pro použití CC.

Struktura CC

Část 1 - Úvod a použitý model

- popis přístupu
- pojmy a model
- požadavky na profil ochrany pro kategorie produktů a bezpečnostní cíle pro konkrétní typy produktů

Profil ochrany
: popisuje prostředí, cíle, požadavky pro kategorii produktů nebo konkrétní typ produktu

Část 2 - Funkční požadavky

Dělí se na

- třídy (Fxx) - seskupení rodin stejného zaměření
- rodiny (Fxx_Axx) - seskupení komponent se stejným cílem
- komponenty (Fxx_Axx.xx) - nejmenší volitelné sada prvků

Třídy funkčnosti F__

- Audit
- Communication
- Cryptographic Support
- Data Protoction
- Identification and Authentization
- Security Management
- Privacy
- Functionality Protection
- Resource Usage
- Trusted Paths

Část 3 - Požadavky zaručitelnosti

Zaručitelnost je ochranou proti

- Špatnému návrhu
- Implementačním chybám
- Neefektivním opatřením nebo mechanismům

Úrovně zaručitelnost
jsou kompatibilní s TCSEC – EAL1 až EAL7.

- EAL4 - nejvyšší pro běžně vyráběné produkty

Třídy požadavků zaručitelnosti

- Configuration Management
- Delivery and Operation
- Guidance Documents
- Life Cycle support
- Vulneralibity Assesment
- Development documentation
- Testing

Část 4 - Registr profilů ochrany

Modely při vývoji

- model bezpectnostnej politky
- funkcna specifikacia
- model architektury
- detailnu model
- implementace

- Modely specifikace lze rozdělit následovně:
  - neformální – zapsaná v přirozeném jazyce, přičemž nepodléhá žádným omezením;
  - poloformální (semiformální) – vyžaduje užití některé omezující notace spolu s množinou konvencí, může mít buď grafickou podobu, nebo být založena na omezeném použití přirozeného jazyka.
  - formální – zapsaná ve formální notaci, která využívá dobře definovaných matematických pojmů.

CEM (Common Evaluation Methodology)

- doplněk k CC
- Popisuje aktivity hodnotitele CC
- Důležité pro vzájemné uznávání.
- Obsah
  - část 1 – úvod a obecný model- terminologie a principy hodnoceni
  - část 2 – metodologie hodnocení
  - část 3 – rozšíření metodologie

Kategorie: Bezpečnost informačních systémů | Státnice 2011

- Stránka byla naposledy editována 16. 6. 2016 v 14:46.