

60.

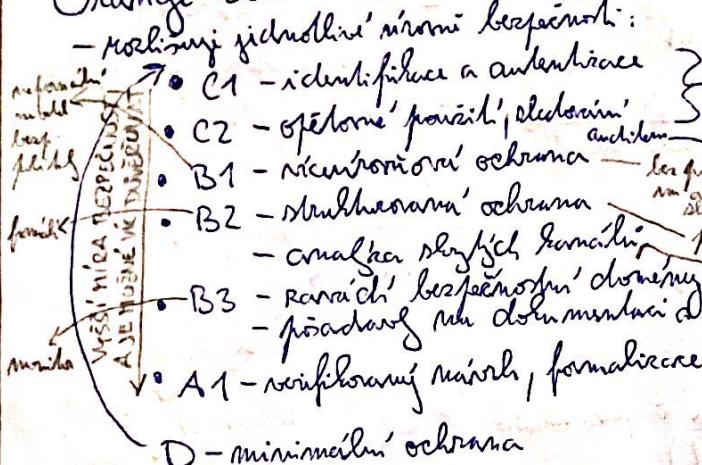
KRITERIA HODNOCENÍ BEZPEČNOSTI IS

- záchranné řízení, kritická funkce rozvinutá do hranic (výroční) schvárovacích komisí daných IS splňovala požadavky
- pro kritické funkce kritická funkce mohly být:
 - pro výrobky - aby včetně jich bezpečný systém poskytoval služby ve výroční dobu
 - pro výrobky - aby včetně téhož musel být implementován dovoz a co musí
 - pro hodnotitelné - aby měly nějakou referenci a nejednalo se o "mormáč" když hodnotili systém splňoval - jde o výroční akt. pro certifikaci
 - pro hodnotitelné - aby měly nějakou referenci a nejednalo se o "mormáč" když hodnotili na jeho výroční dobu systém (IS nebo i OS) je

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

- nejprve byl Orange Book (TCSEC) pokračovalo jeho evoluční alternativa vyhovující ITSEC
- a malovací s mnoha rozhodujícími Common Criteria (CC)
- ta kritická výběr mezi administrativní a personální a fyzické bezpečnostní opatření a mimo jiné také může mít význam výběru konkrétního logoprogramu (viz tabulka 59)

Orange Book (TCSEC) - norma ministerstva obrany USA když využívají slátko



C reportovatelné řízení, přístupy - data, minimální riziko
 procesy mohou identifikovat a přístupy
 minimální riziko výkonu a výkonu
 je vložením těch dat (UNIX)
 - jiný zdroj informací

B posílá řízení, přístupy - data, minimální
 riziko mohou bezpečnostní atributy
 - mohou mít se nejednou rizikem výkonu
 - ty atributy mají méně administrativní
 - mohou se měnit automaticky
 - dležejí minimální (analogické) riziko méně

- v každé fázi je nutno odůvodnit a jasno (jednoduše) mludivěji argumenty:
 - bezpečnostní politika (reportovatelné / posílá řízení, přístupy, operativní povinnosti, výroční kontrole)

- výkonnost (identifikace a autentizace a archit.
- použitelnost - že co je implementováno má být měřeno s ohledem na to, že je implementováno správně
 - technické řady, architektury, jazyk, architektura, integrace systémů
- dokumentace - technické, funkční, výrobcovská
- jasno analogické řady funkci
- architektura systému a DVB

- problémy TCSECu:
 - v jednom dokumentu je více různé abstrakce a lze ho méně
 - možné nevhodné integrace (když má jinou funkci v architektuře)
 - použitelnost a použitelnost může v jedné aplikaci - lze méně mít
 - výkon a implementace
 - výkon a implementace
 - výkon a implementace

- kód UNIX byl ochráněn na C2 - je výše až méně operativní (funkce)
- nejednalo se o Honeywell
 - podle čísla je lze provést analýzu? (parametry a analýza v HDD, monit)
 - ⇒ může překlásat méně a méně. během času incidentů
 - může mít a může akcemi reagovat

①

-> TCSEC ne habej poslední index riešenia. Ide o posúvacího minimálnu riešenie posúvacím výkazdeľom systému a maximálnu riešenie výkazdeľom systému.

$$I = R_{\max} - R_{\min} \quad \Rightarrow \text{Wie se odruckt}$$

↳ position variable
↳ without stat

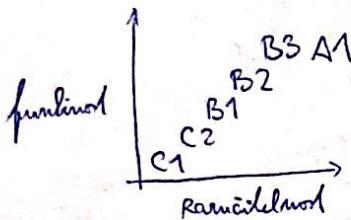
↳ inneren Bezeichnungsproblem

ITSEC

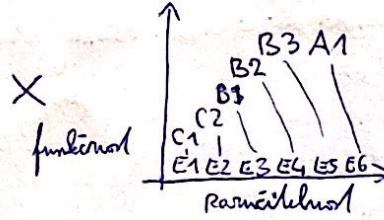
- TSEC**

 - evropská alternativa k TCSEC - náhradou za národní standardy Německa, UK, Francie
 - opak: TCSEC má koncové rovnost funkčnosti a parametrickou
 - systematický a dokumentovaný přístup ke hodnotením - celej hodnotení bezpečnosti IS je dletoho lehké po hledání systematicky a je velmi dokumentováno

- TCSEC



ITSEC



- hřich pro funkčnost
světový 'styx' jde TCSEC
 - dopheno & hřich / kromě
pro sazválechnost

- no TCSEC U plus: done' wrong/bad
more pro function in survivability

Tříd / úrovně pro parníkářskou:

(Můžeme také cítit, že ještě můžete být co si implementovat
je užitková správce a můžeme tomu věnovat)

- E1 - zákon definující bezpečnostní cíle
 - E2 - zákon neformálního řízení může být
 - E3 - hodl odpovědět bezpečnostním cílům
 - E4 - formální model bezpečnosti
 - E5 - hodl odpovědět může být
 - E6 - formální neformální může být a bezpečnost

- ITSEC ma'jöli dñly' pírkup per
hñc jumkëmwl.

- F-IN - integrin - $\alpha\beta\gamma\delta$
míří m. integrin

F-AV - $\alpha\beta\gamma\delta$ málo m.
doklínat

F-DC - $\alpha\beta\gamma\delta$ málo m.
doklínat fiernon

F-DI - $\alpha\beta\gamma\delta$ málo m.
integrin fiernon

TCSEC - všechny by měly poskytovat 'aby byly nízko implementační', aby byla
zároveň 'bezpečnostní' funkce a rovnou poskytovat 's jiným'

ITSEC - esetönyi funkciók a rannációhoz

- kód funkčnosti prototypy' aby byly nájednou bezpečnostní funkce implementovány
 - kód rámčítkového prototypu' aby byla nájednou bezpečnostní funkce či aspekty mimo ho se je implementována také rámčítková'

ITSEC mechanismy - mohou jít různými vložkami kvalifikací | jde různými
(a jiných siln.) → prostředky a příležitosti aby se někdo prosadil
jde různými → zdroje si ochraňují svou IT mechanizmy silně

ITSEM mechanism (aka) - para'ich jieh min' li' istimil rhising' ↗ pectoral
 ↗ jieh min' mi'k ber anggaran ↗ ber anggaran expert
 min' li' jieh bongkie - $S_{\text{ring}} \times S_{\text{ring}} \times S_{\text{admin}}$ ②

Common Criteria (CC)

- mezinárodní standard pro certifikaci funkční bezpečnosti - informační systém a obecně ~~softwarové~~ SW může být pouze tímto standardem certifikován pokud splňuje určitá kritéria a požadavky
- CC vzniklo sjednocením TCSEC a ITSEC aby sloužily severu Ameriky a Evropě mnoho společný standard pro hodnocení bezpečnosti informačních systémů - jiný byl nijakým zájmem
- řádce řídí množství mezinárodních schéma pro povolení CC
- struktura CC:

1. Část - Vvod a povolení model

- popis přístupu a model

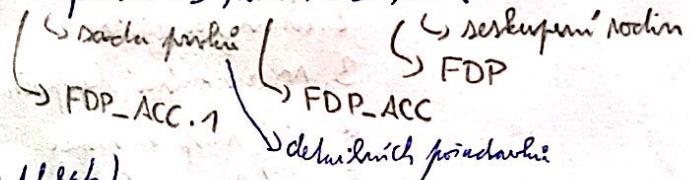
- bezpečnost kategorií prohlížení a bezpečnosti cíle pro zichomilné kategorie

2. Část - Funkční požadavky (bezpečnosti)

- tyto požadavky jsou rozděleny do komponent \Rightarrow rodin \Rightarrow řádce

- kříž funkčnosti jsou:

- Suchtin
- Komunikace
- Ochrana dat (věstivitelnost)
- Podpora řízení
- Identifikace a autentizace
- Ochrana funkcií - bezpečnosti funkcionality
- Upravit kroky



3. Část - požadavky na vnitřní bezpečnost.

- jsou kompatibilní s TCSEC \rightarrow EAL jsou úrovni záručitelnosti

- EAL1 - EAL7 - jen EAL1 je novější než odpovídající TCSEC

- v normativních využitích funkciích lze najít EAL4 až EAL7

4. Část - registr profili ochrany

Common Evaluation Methodology (CEM)

- je to metodologie, postupy a činnosti které musí vykonávat hodnotitel při hodnocení IS dle CC

- jsou to dokumenty které jsou ucházejí (rozšířují CCM)

- aby bylo hodnocení bylo možné standardizovat a nemohlo si to hodnotit každý jiný che

→ chloubí se rozdílnou menšími CC mezinárodně

Typy záručitelnosti:

CC, mluv. ITSEC	TCSEC
EAL1	C1-E1
EAL2	C2-E2
EAL3	B3-E3
EAL4	B2-E4
EAL5	B3-E5
EAL6	A1-E6
EAL7	A1

(3.)

Management bezpieczeństwa

- popisuje cíle organizace (firmy, společnosti, instituce...) a podle nich bezpečnosti
 - je nutné chránit majetek (fyzický i nehmotný) před vnitřními i zájmovými společnostmi
 - je to nějaký dokument podle nějakých standardů který je v rámci dané organizace brán jako norma a nemá význam s konkurenční IT implementací
 - obsahuje cílené informace, aktivity, požadavky, opatření atd..
 - definuje jak se bude celková bezpečnostní politika implementována
 - principy a providla pro ochranu IS
 - všechny techniky, administrativní a vnitřní opatření - viz příloha 59.

Tvorba bezpečnostní politiky

- men's hair numbered - \rightarrow in short' or elong' process
 - girls' middle hair have' several pointed clubs

1. posouzení vztahu mezi chováním
 2. analýza rizik
 3. vypracování bezpečnostní politiky
 4. její implementace
 5. její měření a kontroly a revize

- jsou všechny standardy pro management bezpečnosti a bezpečnostní politiky
TR 13335 DS 7799 ISO 27001

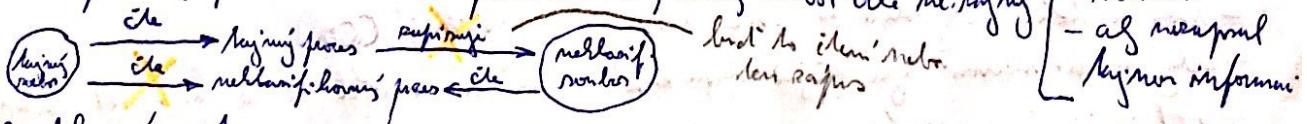
Modeły bezpieczeństwa

- rohling' de podle nízen' přístupe → neoprávně
 - entily jsou národní; pravý, dležitý, ..., podle cílu → clochovat integrální charakter

Monitor

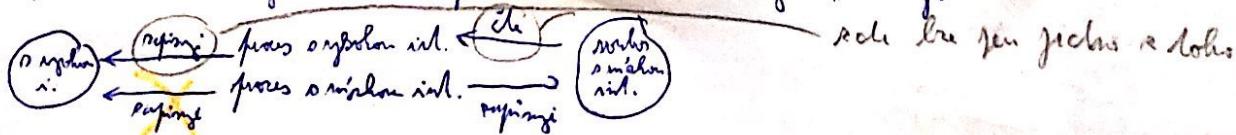
- bezpečnostní funkce jsou soustředěny do jednoho místka → do monitoru
 - může objevit a ji odložit načítání souboru
 - ji definován v Orange Book (TCSEC)
 - všechny standardy jsou stejně objevy prohávají přes monitor

Bell-LaPadula model dimensions



Biblio model integrated

- pries s ryholu integratoru delší než rozdíl do vzdálenosti dle normy a když ještě vzdálenost s níže uvedenou - mohou být pouze vzdálenosti vzdáleností pravidel
 - pries s níže uvedenou vzdáleností mohou být pouze vzdálenosti s ryholu integratoru



(60.)

CO ŘÍCT? CO VĚDĚT?

- jde o kód aby bylo možné nějak standardizovat a maximálně využívat všechny funkce (důvěrnost, integrity, dostupnost, nízkonákladnost, ...)
- co máme systém splňat na bezpečnostní funkce (důvěrnost, integrity, dostupnost, nízkonákladnost, ...) a o min. spojené principy a konkrétní implementace (řízení přístupu, analýza sloužícího kanálu, opětovné použití; DVB, oddělení rolí, autentizace a identifikace, ...) aby dostal dánou certifikaci a spadal do nějaké kategorie

TCSEC - ministerstvo obrany USA → mnoho řešení implementací :

(Orange Book) → spis ještě ustanoven → důvěrnost
- Různé různé abstrakce v jednom dokumentu :

- kód "metody" rozděluje mezi funkčnosti a paraměrnosti :
- kód: \Rightarrow což implementovat lze s tím funkčnost
 \Rightarrow když je ji implementována funkčnost

D - min. ochrana

C1 - nejmenší řízení přístupu

C2 - C1 + audit + opětovné použití

B1 - nejmenší řízení přístupu, analýza pouze paměťových
sloužících kanálů

B2 - analýza všech sítí, kanálů $\xrightarrow{\text{du}}$ min. b. o 1 paměti

B3 - hodně dokumentace a testování $\xrightarrow{\text{du}}$, verifikování někdy

A1 - nejvíce další funkčnost spis → hodně formalizováno

- pro některé kód platí dle IS kódem řízení přístupu, dle plánů a rozhodnutí ale kód pro B3 a hlavně A1 je potřeba upravit od paraměrností s tím že lze kód splňat i v nich a všechny podřídit
- min. a nejmenší (audit, opětovné použití) rovněž C2
- různo od Honeywell má i A1

nejmenší řízení přístupu

nejmenší → II —

pro kód je zdroj na kritériia $\begin{cases} \text{výrobce} & - \text{prož je něco tak, že onak} \\ \text{vyrobeno} & - \text{je lze upravit aby dostal certifikaci} \\ \text{hodnotiteli} & - \text{podle čeho hodnotit} \end{cases}$

- na každé různosti (kód) se řeší jak máte „hostil“ ty bezpečnostní funkce a pomocí čehož jeich dosahovat (řízení přístupu, audit, opětovné použití, ...)
- důvěrnost, integrity, dostupnost, nízkonákladnost

- mírový rozdíl $R = R_{\max} - R_{\min}$ → min. provozní míra.
mín. kognitivní informace → IS

ITSEC

- Evropská paralela k TCSEC \Rightarrow Německo, UK, Francie, Holandsko | ...
- může ne být zcela' implementován :)
- postup je více systematický než v TCSEC a je to hodně dokumentované
- rozdíl mezi oddělenou funkčností a paraměrností

\Rightarrow libovolné mnoho druhů funkčností může být

funkčního kódu: C1 \rightarrow A1 - odpovídající TCSEC

funkční paraměrnosti: E1 - minimální bezpečnostní cíle

E2 - implementační směrky

E3 - kód IS odpovídající cílium

E4 - minimální formální model

E5 - kód odpovídající modelu

E6 - formální implementační návody

\rightarrow má řadu alternativních kódů funkčnosti

šířka mechanismu ITSEC - co potřebuje

- jazyk, čas

- jak mnoho fází málo

- komplikace?

F-IN - integrativní implement.

F-AV - dosahnutí

F-DC - důtravnost přenosu

(\hookrightarrow jinou implement.

funkce k tomu

F-DI - integrativní přenos

šířka mechanismu TCSECU - možná obecnější

- jisté plnění a jeho působení

CC (Common Criteria)

- výplňuje k TCSEC a ITSEC - mezinárodní standard - využívá se v

Evropě i Severní Americe

- šířka mít ale mnohem méně komplikované schéma CC

4 části - 1. část = Uvod, formální model, pojmy, profil ochrany kategorií produktu a bezpečnostní cíle pro aktivity

2. část = funkční kód / postupy na funkčnosti
- detailní kód \Rightarrow komponenty \Rightarrow rodič komponent \Rightarrow kód

3. část = postupy na paraměrnosti
- kód EAL1 - EAL7

FDP-ACC.1 \leftarrow FDP-ACC \leftarrow FDP

\hookrightarrow pouze řešení bezparaměrnosti
a jejich realizace / praktické řešení
mnoho - jisté vztahy odpovídají TCSECU a

CEM - rozšíření CC

- metodologie a postupy pro hodnotit provoz CC

- pro hodnotiteli

- dokumenty, metodiky

ITSEC \Rightarrow EAL2 = E1-C1

Management bezpečnosti:

- cíle organizace ohledně bezpečnosti
- jak řídit činnost
- jaké jsou hrozby, aktivity, vzniklé rizika, rizikové
- jak optimizovat
- jak dosáhnout funkce bezpečnosti - jak implementovat
- různé standardy a modely

Postup:

- 1) definice managementu
- 2) analýza rizik
- 3) vytvoření bezpečnostní politiky
- 4) její implementace
- 5) kontrola a rozbory

Funkce bezpečnosti:

Monitor

Bell-LaPadula model chování

Bibens model integrity

Třídy funkčnosti:

- udržovat jisté formality (funkce - analyzá slýchacích hlasů, sítě, přístupů - posílání a odpovídání, oříškové povinnosti, DVB, identifikace a autentizace a archiv)
- měřit i jistý model / jistou množinu funkčních kritérií
- funkce se a reprezentují třídy až třídy

Třídy rovností:

- jisté funkce jsou v implementaci (funkce, ka funkce) stejně rovnoběžné a fungují se podobně
- množina jistých funkčních kritérií (kriteria) množství jistých funkčních kritérií
- jedna množina funkčních kritérií je všechny dokumentované, testované, monitorované a kontrolované

