Více úrovňové informační systémy a jejich certifikace podle zákona č.412/2005 Sb.

Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení a o certifikaci stínicích komor

NBÚ, Odbor informačních technologií
a.maskova@nbu.cz, p.adler@nbu.cz

Bezpečnostní provozní módy

- vyhrazený
- s nejvyšší úrovní
- víceúrovňový

definovány v předpisech NATO, EU, národních (vyhláška č. 523/2005 Sb.)
prvé dva jsou jedno- úrovňové

Bezpečnostní provozní mód víceúrovňový

- **Bezpečnostní provozní mód víceúrovňový je takové prostředí, které umožňuje v jednom informačním systému současné zpracování utajovaných informací klasifikovaných různými stupni utajení, ve kterém nemusí všichni uživatelé splňovat podmínky přístupu k utajovaným informacím nejvyššího stupně utajení, které jsou v informačním systému obsaženy, přičemž všichni uživatelé nemusí být oprávněni pracovat se všemi utajovanými informacemi.**

Bezpečnostní funkce

- jednoznačná identifikace a autentizaci uživatele informačního systému, ochrana důvěrnosti a integrity autentizační informace,
- volitelné řízení přístupu k objektům informačního systému na základě přístupových práv uživatele a jeho identity nebo členství ve skupině uživatelů,
- nepřetržité zaznamenávání bezpečnostně relevantních událostí do auditních záznamů a zabezpečení auditních záznamů před neautorizovaným přístupem, zejména modifikací nebo zničením

Bezpečnostní funkce

- možnost zkoumání auditních záznamů a stanovení odpovědnosti jednotlivého uživatele,
- ošetření paměťových objektů před jejich dalším použitím, zejména před přidělením jinému subjektu informačního systému, které znemožní zjistit jejich předchozí obsah,
- ochrana důvěrnosti dat během přenosu mezi zdrojem a cílem, a dále
- **povinné řízení přístupu**

Povinné řízení přístupu

- Funkce povinného řízení přístupu subjektů IS k objektům IS musí zabezpečit
  - trvalé spojení každého subjektu a objektu IS s bezpečnostním atributem, který
    - pro subjekt IS vyjadřuje úroveň jeho oprávnění
    - pro objekt IS jeho stupeň utajení,
  - ochranu integrity bezpečnostního atributu,

Povinné řízení přístupu

- výlučné oprávnění bezpečnostního správce IS k provádění změn bezpečnostních atributů subjektů i objektů informačního systému

- přidělení předem definovaných hodnot atributů pro nově vytvořené objekty IS a zachování atributu při kopírování objektu IS

Povinné řízení přístupu

- bezpečnostní funkce povinného řízení přístupu musí zajistit tyto zásady
  - subjekt informačního systému může číst informace v objektu informačního systému pouze tehdy, je-li úroveň jeho oprávnění stejná nebo vyšší než stupeň utajení objektu informačního systému,
  - subjekt informačního systému může zapisovat informaci do objektu informačního systému pouze tehdy, je-li úroveň jeho oprávnění stejná nebo nižší než stupeň utajení objektu informačního systému,

Povinné řízení přístupu

- přístup subjektu IS k informaci obsažené v objektu IS je možný, jestliže jej povolují jak pravidla povinného řízení přístupu, tak pravidla volitelného řízení přístupu,
- IS v bezpečnostním provozním módu víceúrovňovém, musí být schopen přesně označit stupněm utajení utajované informace vystupující z IS a umožnit přiřadit stupeň utajení utajované informaci vstupující do IS,
- bezpečnostní funkce musí být realizovány identifikovatelnými programově technickými mechanismy, dokumentovány tak, aby bylo možné jejich nezávislé prověření a zhodnocení.

Bellův a LaPadulův formální model bezpečnostní politiky

- Bell D.E., La Padula L.J., 1976, zpráva MITRE Corporation, vyvinut pro DoD US
- vliv na TCSEC
- vliv na ITSEC
- vliv na profily v CC

Bellův a LaPadulův formální model bezpečnostní politiky

- bezpečnost formálně popsána a dokázána
- stavový model - stav je bezpečný pokud je v souladu s bezpečnostní politikou pro přístup subjektu k objektu; porovnává se úroveň prověření subjektu a stupeň utajení objektu + „need-to-know“ subjektu k objektu; přechod do dalšího stavu zajišťován tak, že nový stav je opět bezpečný
- základní zásady bezpečnostní politiky pro MAC:

  - Simple Security Condition: subjekt nesmí číst z objektu vyšší bezpečnostní úrovně (no read-up)

  - * Property: subjekt nesmí zapisovat do objektu nižší bezpečnostní úrovně (no write-down)

  - Discretionary security property (dle přístupových práv, jako v jednoúrovňovém IS)

Základní dokumenty

- TCSEC (Trusted computer System Evaluation Criteria - Orange Book), rok 1983, update 1985, třídy B1(Labeled Security Protection), **B2**, B3
- ITSEC (Information Technology Security Evaluation Criteria), rok 1990 a 1991, funkční třída F-B2 odpovídá třídě B2 s úrovní důvěry E4 (pro F-B1 úroveň E3)
- CC, profily zahrnující povinné řízení přístupu, hodnocení produktu min. na úrovni EAL4

Bezpečná realizace

- víceúrovňový operační systém ohodnocený podle některých z kritérií bezpečnosti (CC)
- na aplikační úrovni – obtížné navrhnout, implementovat, poté prokázat bezpečnost
- využití kryptografické ochrany - obtížnost návrhu, implementace, prokázání bezpečnosti

Bezpečná realizace

- aktuálně neznáme v oblasti utajovaných informací realizaci víceúrovňového IS v NATO ani EU
- některé operační systémy hodnocené podle CC mají modul zajišťující povinné řízení přístupu (Mandatory Access Control- MAC)
- režie na správu víceúrovňového systému je údajně vysoká, funkce MAC není využívána

Bezpečná realizace

- IBM z/OS v módu Labeled Security mode
- některé UNIX/LINUX systémy mají zabudováno kromě volitelného i povinné řízení přístupu, které ale musí být aktivováno:

  - Free BSD 8.2 Release (při kompilaci se přidá MLS modul, volí se úrovně)
  - Red Hat Enterprise Linux Ver. 5 on IBM Hardware
  - AIX 6 ver. 6100-00-02
  - Solaris 10 Release 11/06 Trusted Extensions
  - aj.

Bezpečná realizace

Poznámky

- stěžejním problémem je přesná implementace Bell-LaPadula modelu, zejména udržení integrity atributů subjektů a objektů a neobejitelnost pravidel pro přístup
- některé certifikované IS v bezpečnostním provozním módu s nejvyšší úrovní využívají labelů s označením stupně utajení a kategorie informace připojených k některým objektům (např. e-mailová zpráva); to z nich ještě nedělá víceúrovňový systém
- přímo na OS Windows postavit víceúrovňový systém nelze

Dotazy ?