MI-PB-20

Úrovně bezpečnosti v informačních systémech: pravidla a politiky pro počítače, OS a sítě.

Systémová bezpečnost:
Ochrana:

- **Důvěrnosti dat:**
  - Zabraňuje neautorizovaným subjektům interagovat s prostředky
  - Hrozba: crackování šifrovaných dat, man-in-the-middle, spyware
- **Integrity dat:**
  - Zabraňuje nežádoucím modifikacím dat
  - Hrozba: injekce malwaru do webserveru a do webových stránek, falšování záznamů
- **Dostupnosti dat:**
  - Při autorizovaném přístupu jsou data dostupná na dané výkonostní úrovni
  - Hrozba: (D)Dos, ransomware, odpojení serverovny od elektřiny

Všechny systémy operují v **nepřátelském prostředí**

Systémová bezpečnost **není absolutní** - Žádný systém není perfektně zabezpečen

Politiky

Bezpečnostní politika: požadavky a cíle na systém/síť, aby byla dosažena jejich bezpečnost (např. Alice může číst soubor F)

Model hrozeb: předpoklady o tom, co útočník může dělat (např. hádat hesla)

Model bezpečnosti: popis, jak splnit požadavky dané politikou

Mechanismy: prostředky, které systém poskytuje, které pomáhají vymáhat politiku (uživatelské účty, hesla, oprávnění)

Výsledný cíl systémové bezpečnosti: útočník z modelu hrozeb nesmí nijak narušit bezpečnostní politiku

Vrstvy bezpečnostní politiky:

- Vrstva 1: **Základní politika**
  - Dlouhodobě plánovaná (na několik let)
- Vrstva 2: **Operační pravidla a standardy bezpečnostních opatření**
  - Pravidla a standardy k zajištění informační bezpečnosti specifikované v základní politice
  - Střednědobé (jednou ročně)
- Vrstva 3: **Procedury a pokyny**
  - Speficické procedury a činnosti pro plnění pravidel
  - Krátkodobé plány (několik ročně)

Rizika

Risk Management:

- Bezpečnější systém $\Rightarrow$ menší riziko
- Nezabezpečený systém $\Rightarrow$ manuální audity, kontroly
- Vyšší cena útoku $\Rightarrow$ odrazení útočníka

Analýza rizik:

- **Asset:** cokoliv cenného pro organizaci, co by se mělo chránit
- **Hrozba:** potenciální událost, která může mít nežádoucí následek pro organizaci nebo asset
- **Zranitelnost:** slabina v assetu nebo v opatření
- **Exposure:** náchylnost ke ztrátě assetu kvůli hrozbě
- **Riziko** = hrozba $\times$ zranitelnost
- **Opatření:** cokoliv, co odstraní nebo zmenší zranitelnost
  - Fyzická: psi, ploty, zámky
  - Administrativní: zaměření na personál a bussiness praktiky (školení, audity, vymezení povinností)
  - Logická: logická izolace, segmentace (VLAN, virtualizace), access control, authentication, authorization, logging, auditing

Security modelling

Trusted computing base: komponenty zodpovědné za dodržování politiky

Security perimeter: hranice oddělující TCB of zbytku systému
Reference monitor: část TCB, která ověřuje přístup ke každému zdroji
Aby TCB bezpečná, musí splňovat:

- úplnost (všichni přistupují přes TCB)
- izolace (TCB cháněná před neautorizovanou změnou)
- ověřitelnost (TCB splňuje návrhová specifika)

Kdo nastavuje politiku:

- Majitel objektu ⇒ **discretionary access control**
  - Např. ACL:
    - Linux ACL (klasická oprávnění)
    - Windows ACL:
      - Discretionary (DACL): kdo má oprávnění přístupu k objektu
      - System (SACL): jaké operace jakých uživatelů se mají logovat
- Politika celosystémová ⇒ **mandatory access control** (např SELinux)
- Politika určená rolí uživatele ⇒ **role-based access control**

Každý proces izolován vynucováním access bounds (limitů na použitelné paměťové adresy a prostředky systému)

Multilevel security:

- Objekt je buď *unclassified*, *confidential*, *secret* nebo *top secret*
- Uživatel musí mít příslušná oprávnění

Multilateral security:

- Bere v potaz různé (někdy konfliktní) požadavky na bezpečnost, hledá mezi nimi rovnováhu
- Např. uživatelé z různých geografických regionů nemůžou vzájemně přistupovat ke svým datům

Pozitivní model: definice, co vše je povoleno (whitelisting)
Negativní model: co vše je zakázáno (blacklisting), obtížnější na definování, nelze zachytit 100 % hrozeb

Model Bell-LaPadula:

- Multilevel
- Vynucuje důvěrnost, žádná integrita
- Hlavní cíl: zabránit kompromitaci tajných dat

- Každý subjekt a objekt mají svou úroveň
- Simple security property: žádný proces nesmí číst data z vyšší úrovně
- *-property: žádný proces nesmí zapsat do nižší úrovně
- Příklad: SELinux (pravidla vynucená kernelem, uživatel nemůže vypnout)

Model Biba:

- Vynucuje integritu, žádná důvěrnost
- Hlavní cíl: zabránit neautorizované modifikaci
- Simple integrity property: subjekt nesmí číst z nižší úrovně integrity
- *-integrity property: subjekt nesmí zapsat do vyšší úrovně integrity
- Příklad: Windows Integrity (různé úrovně)

Model Chinese wall:

- Multilaterální: kombinace discretionary a mandatory
- Objekty (soubory): obsahují informace o 1 company
- Company group: objekty o jedné konkrétní company
- Conflict class: skupiny objektů pro soupeřící companies
- Simple Security rule: subjekt může přistupovat k informacím z libovolné company, pokud nikdy nepřistupoval k nějaké jiné company ze stejné konfliktní třídy
- *-property: zápis pouze pokud povolen přístup simple security rulem a nelze číst žádný jiný objekt z jiné company
- Příklad: společnosti poskytující služby třetím stranám (finanční, konzultace, audit)

Clark-Wilson model:

- Navržen pro komerční sféru
- Vynucení integrity
- Koncept oddělení povinností
- 4 základní koncepty:
  - autentizace, access control: identita všech uživatelů musí být autentizována
  - audit: modifikace logovány
  - integrita, transakce: uživatelé manipulují s daty pouze předepsanými způsoby, pouze legitimní přístup je povolen
  - oddělení povinností: unikátní asociace uživatelů a jejich činností, každý uživatel má množinu programů, které může spustit
- Constrained Data Item: objekt, jehož integrita je hlídaná
- Transformation Procedure: jediné procedury, které mohou modifikovat nebo vytvářet CDI

- Integrity Verification Procedure: ověření udržování integrity CDI
- Oprávnění zakódována jako trojice $(\text{user}, \text{TP}, \{\text{CDI set}\})$
- Pravidla:
  - Certification:
    - Systém musí mít IVP pro všechny CDI
    - Všechny TP musí zaručit zachování integrity
    - Přiřazení TP uživatelům musí uspokojit oddělení povinností
    - TP musí být logované
    - TP provedená na unconstrained data item musí vyústit v platný CDI
  - Enforcement:
    - Pouze certifikované TP mohou manipulovat CDI
    - Uživatel může přistoupit k CDI pouze před TP, pro kterou je autentizován
    - Identita každého uživatele spouštějícího TP musí být autentizována
    - Pouze admin smí vytvářen TP a specifikovat jejich autorizace
- Příklad: databáze, Windows NT