Principy operačních systémů

zpracoval Martin Kuba

16. května 1995

Obsah

1 Bezpečnost IS

Při uvažování o bezpečnost informačního systému je nutno zvážit všechny následující věci:

- řízení přístupu
- kryptografie
- zvládnutí rizik
- zabezpečení chodu činnosti
- klasifikace dat
- bezpečnostní uvědomění
- počítačová/systémová bezpečnost
- telekomunikační bezpečnost
- bezpečná architektura organizace
- právní aspekty
- vyšetřování – příčiny a původy incidentu
- bezpečnost aplikačních systémů
- fyzická bezpečnost
- provozní bezpečnost
- etická kriteria
- stanovení bezpečnostní politiky organizace
- hodnocení bezpečnosti

Informační systém tvoří

HW — CPU, paměť,...

SW — aplikace, OS

data — výsledky, údaje v databázích

lidé — uživatelé, personál

Nadefinujme si některé pojmy:

bezpečnostní politika — normy, pravidla a praktiky (zpracování, distribuce, citlivé informace)

objekt IS — pasivní entita

subjekt IS — aktivní entita (osoba, proces) autorizovatelná pro získání informace nebo změnu stavu objektu

autorizace — určení, zda je subjekt důvěryhodný z hlediska jisté činnosti

důvěryhodný IS/objekt/subjekt — o kterém se věří, že splňuje svoji specifikaci v souladu s bezpečnostní politikou

bezpečný IS/objekt/subjekt — na který se můžeme spolehnout

nebezpečí —

- útoky lidského činitele

- chyby lidských činitelů
- přírodní katastrofy
- poruchy a chyby HW a SW

útok — využití zranitelného místa ke způsobení škod

Typy útoků:

přerušení — ztráta dat, znepřístupnění

odposlech — kopie

změny — přidání funkcí do programů, změny dat

přidání hodnot

Bezpečnostní cíle a jejich dosažení:

- funkce prosazující bezpečnost
  - ⋆ identifikace a autentizace (utajování)
  - ⋆ řízení přístupu
  - ⋆ účtovatelnost (audit)
- bezpečnostní mechanismus — logika nebo algoritmus, kterým HW/SW imlementuje funkce prosazující bezpečnost

2 Řízení přístupu

2.1 Autentizace uživatelů

pozitivní identifikace s jistým stupněm záruky

- uživatel něco zná
  - ⋆ heslo
  - ⋆ PIN (Personal Identification Number)
- uživatel něco má
  - ⋆ klíč k terminálu
  - ⋆ smart card
- uživatele něco jedinečně charakterizuje
  - ⋆ otisk prstu
  - ⋆ vzorek žilek v sítnici
  - ⋆ geometrie ruky
  - ⋆ vzorek hlasu (pozor na nemoci !)
  - ⋆ frekvence psaní na klávesnici
  - ⋆ fotografie

2.1.1 Hesla

útok hrubou silou – vyzkoušením všech možných kombinací znaků – nemá moc šancí na úspěch, už při osmiznakovém heslu by trval několik desítek let i při vyzkoušení tisíců hesel za sekundu

útok na pravděpodobná hesla — vyzkoušení křestních jmen, slov ze slovníku, ...

útok na hesla související s uživatelem — jméno manželky, rodné číslo, číslo kanceláře

útok nalezením seznamu hesel — hesla jsou uložena jako

- srozumitelný text s chráněným přístupem je zjititelný
  - ⋆ z tabulky otevřených souborů
  - ⋆ dumpingem paměti
  - ⋆ zcizením archivní kopie
- šifrovaný text
  - ⋆ někdy se musí dekódovat
  - ⋆ pokud ne, zakódovat a porovnávat šifrované texty

útok přímým dotazem —

- heslo napsané na terminálu
- sdílené soubory – sdílení hesla
- trojský kůň

Pravidla pro práci s hesly:

- snadno zapamatovatelná a špatně uhádnutelná
- co nejširší abeceda
- dlouhá hesla
- ne běžná jména a slova (běžná slova tvoří asi 0.05% možných řetězců)
- nepravděpodobná hesla
- často měnit
- nikde nezapisovat, nikomu nesdělovat
- konečný počet pokusů o zadání hesla
- audit pokusů o zadání hesla
- nezadávat počáteční heslo veřejně
- v systému uchovávat šifrovaně

Nejlepší zkušenosti jsou s hesly, která jsou skutečná slova proložená nepísmenými znaky, protože se lépe pamatují a přitom k jejich nalezení je nutný útok hrubou silou přes všechny kombinace znaků.

2.1.2 správa objektů

Centralizovaná správa — jeden správce v organizaci

- výhody – přísné řízení, přehled, konzistence
- nevýhody – vysoká (časová) režie

Decentralizovaná správa — objekt zpravuje jen jeho vlastník

- výhody – rychlost
- nevýhody – vysoká zodpovědnost vlastníka, není celkový přehled, komunikace se správci nemusí být konzistentní, špatně se prosazuje bezpečnostní politika

Mechanismy pro řízení přístupu k objektům

- **heslo**/šifrovací klíč (HP-1000)
- **bitové příznaky oprávnění** (Unix) rwx pro *owner, group, others* – nelze zajistit důvěrnost, protože někdo ze skupiny si může udělat kopii a tu pak dát k dispozici ostatním. Také nelze propůjčit práva jen jednomu konkrétnímu uživateli.
- **model WAX/VMS** — bitové příznaky rwx jsou pro *system, owner, group, world* a pak seznam *kdo-rwx*.
- **seznam oprávnění** (OS MULTICS) – seznam, kdo může číst, seznam, kdo může psát, ...
- **data flow control** – klasifikace subjektů a objektů

klasifikační úroveň	úroveň autority
veřejné	ostatní
důvěrné	vedoucí
tajné	náměstci
přísně tajné	vedení

  třídy bezpečnosti jsou dvojice (C, A), kde C je množina úrovní autorit a A je klasifikační úroveň.

  Data smí téct z (C, A) do (C', A') jsetliže $C \subseteq C'$ a $A < A'$.

  (ostatní, veřejné) $\Rightarrow$ (ostatní, důvěrné)
  (vedoucí, tajné) $\Rightarrow$ ({vedoucí,vedení},přísně tajné)
  (vedoucí, tajné) $\not\Rightarrow$ (vedení, přísně tajné)

  Data flow control je *jediný* spolehlivý způsob ochrany opravdu zajišťující bezpečnost.

- omezená uživatelská prostředí orientovaná na menu – vysoká režie, ale účinné

2.1.3 Autentizační zařízení

Smart card – chytrá karta provádí funkci E, uživatel se vůči kartě prokáže PIN, počítač dodá čas t a karta pošle počítači $E(PIN + t)$. K proniknutí do systému je tedy nutné zjistit PIN a zcizit kartu, což okradený uživatel ihned zjistí.

2.2 Autentizace a kryptografie

Tato kapitola je shodná s kapitolou o kryptografii v "Distribuovaných algoritmech a počítačových sítích", jedná se o symetrické (např. DES) a asymetrické (např. RSA) šifrování a o digitální podpis.

3 Kriteria bezpečnosti IS

Zavedení normy pro kriteria bezpečnosti je výhodné pro *uživatele*, protože ví, co má od systému čekat, pro *výrobu*, protože ví, co má implementovat, a pro *certifikační úřad*, protože má základ pro vydávání certifikátů.

Proto byly v USA vydány normy pro bezpečnost IS:

- Orange Book – TCSEC
- Grey Book – o databázích
- Raspberry Book – o sítích

Rozdělení do tříd bezpečnosti vychází z hodnocení *bezpečnostní politiky, účtovatelnosti, míry záruk a dokumentace.*

D — hodnocený, ale nezařazený IS, nespadá do žádné z vyšších kategorií

C1 — volitelné řízení přístupu, nepovinná ochrana bezpečnosti

- izolovatelnost prostředí uživatelů
- volitelné řízení přístupu k datům přístupovými právy
- ochrana před neúmyslnými a mírnými útoky
- neexistují zjevná zranitelná místa
- všechna data mají stejný stupeň utajení

C2 — zpřísnění nepovinné ochrany

- totéž co C1
- jednoznačná identifikace a autentizace uživatelů
- audit
- ochrana při opětném použití objektů (vymazat uvolňovanou paměť nebo místo na disku)

B1 — povinné řízení přístupu

- C2 a odstranění nedostatků zjištěných testováním
- neformální (slovně stanovená) bezpečnostní politika
- povinná definice přístupových práv *pojmenovaných* objektů a subjektů
- klasifikace dat a všech informací exportovaných z IS
- řízení přístupu na základě klasifikace objektů IS

B2 — strukturovaná ochrana

- B1
- formální definice BP, lze formálně testovat a dokazovat
- povinná definice přístupových práv *všech* objektů a subjektů
- je provedena analýza skrytých kanálů (kanál přenosu informací nesplňující BP)
- strukturalizace IS na kritickou a nekritickou část
- zesílený mechanismus autentizace
- lze používat důvěryhodná zařízení a funkce s certifikovanými vlastnostmi
- odolnost proti běžným útokům

B3 — bezpečnostní domény

- B2
- autorizaci prověřují *správci prostředků* odolní fyzickému útoku

- správce prostředků musí být snadno testovatelný a analyzovatelný
- správci prostředků mají jednoznačně určenou odpovědnost
- audit umožňuje on-line detekci nebezpečných stavů
- lze použít bezpečné zotavení po poruše nebo útoku
- odolnost i proti silnému úmyslnému útoku

A — verifikovaný návrh

- B3
- formálně verifikováno splnění funkčních požadavků a analýza skrytých kanálů
- existuje formální model BP a formální důkaz konzistence a adekvátnosti
- návrh IS se provádí pomocí formálních specifikací shora dolů
- neformálně se prokáže, že implementace odpovídá specifikaci

V Evropě byla zavedena podobné třídy bezpečnosti E0 až E6, přičemž zhruba odpovídají americkým takto:

Evropa	U.S.A.	popis
E0	D	nedostačující důvěra
E1	C1	neformální popis IS a specifikací
E2	C2	testování funkcí
E3	B1	hodnocení implementace mechanismů
E4	B2	formální popis BP
E5	B3	prokázána korespondence s implementací
E6	A	formální popis funkcí zajišťujících bezpečnost

4 Počítačové viry

trojský kůň — zdánlivě užitečný program, který navíc provádí nějakou zlomyslnou činnost

počítačový virus — vkládá sám sebe do jiných programů

síťový červ — samostatný program šířící se komunikačními službami sítí (rexec, rsh, rlogin, E-mail)

4.1 Druhy virů

- bootblock viry — v zaváděcí oblasti disku
- přepisující souborové viry — přepíší kus spustitelného souboru
- nepřepisující souborové viry — přidají se na konec programu nebo do datové části vyplněné nulami apod.
- adresářové viry — modifikují strukturu adresářů a tak se ukryjí
- companion viry — k souboru `PROG.EXE` vytvoří ve stejném adresáři soubor `PROG.COM` s virem a využívají přednosti `.COM` souborů při spuštění

4.2 Druhy antivirových programů

- generický monitor — kontroluje rezidentní programy, operace s COM/EXE, formátování
- kontrolor integrity — zapamatovává si kontrolní součty a občas je kontroluje
- vyhledávací programy — databáze vzorků kódu viru