

Auditovatelnost

- vystopovatelnost
- vedení záznamů
- pass through problem

Autentizace pro počítače

- metoda jednorázových hesel

Autentizace v prostředí databáze

- SRDB jako uživatelský proces

Autentizace v síti

- jednotné přihlášení (single sign on)
- centrální správa uživatelů / synchronizace

Autorizace, úroveň ochrany objektu

- žádná ochrana
- izolace
- sdílení všeho nebo ničeho
- sdílení s omezenými přístupy
- sdílení podle způsobilosti
- limitované použití objektů

Bell-LaPadula model

- popis bezpečných přesunů informací
- bezpečnostní třídy
- vlastnost jednoduché bezpečnosti $C(O) \leq C(S)$
- *-vlastnost $C(O) \leq C(P)$

Bezpečnost fyzické přenosové vrstvy

- pasivní/aktivní
- kabely (wiretaping)
- mikrovlny
- satelitní přenos
- celulární rádio

Bezpečnostní architektura OS (ring, vrstvý)

- layered design – vrstvy, využívání/poskytování služeb
- kruhová (ring) – ochrana segmentu, závora kruhu $\langle b_1, b_2, b_3 \rangle$, access bracket, call bracket

Bezpečnostní kernel

- oddělení od zbytku
- jeden kus kódu
- kernel malý
- snazší testování
- veškeré žádosti skrz kernel

Bezpečnostní modely obecně

- požadavky
 - utajení
 - integrita
 - dostupnost
 - anonymita
 - nepopiratelnost
 - včasnost
 - současnost
 - autenticita
 - pseudonymita
- jednoúrovňové – ano/ne
- víceúrovňové – stupně senzitivity, původ přístupu

Bezpečnostní politika

- Životní cyklus bezpečnostní politiky
 - identifikace aktiv
 - vytipování hrozeb
 - návrh řešení
 - vyhodnocení
 - implementace
 - verifikace
 - administrace
 - reakce na změny

- statement – záměr bezp. (podpis top management)
- politika a principy bezpečnosti
 - popis cílů bezpečnosti
 - zodpovědnost
 - závazky za udržení bezpečnosti

Biba model

- duální model k Bell-LaPadula
- integrita dat, integritní bezpečnostní třídy
- vlastnost jednoduché integrity $I(O) \leq I(S)$
- *-vlastnost $I(O) \geq I(P)$

Biometricky

- identifikace lidí na základě osobních charakteristik
- verifikace hlasu
- verifikace dynamiky podpisu
- verifikace otisků prstů
- geometrie ruky
- obrazy sítnice
- další biometricky

BS 7799

- organizační norma
- obecný popis činností pro zajištění bezpečnosti IS
- budování bezpečnosti shora dolů
- proces tvorby bezpečnosti:
 - definujte zásady bezpečnosti → politika
 - stanovte rozsah ISMS → rozsah
 - proveďte hodnocení rizik → hodnocení
 - zaveďte řízení rizik → seznam akcí k provedení
 - zvolte cíle řízení a opatření k implementaci → zdůvodnění výběru
 - vytvořte směrnici aplikovatelnosti → směrnice
- pokrývá tyto oblasti
 - bezpečnostní politika
 - klasifikace a řízení aktiv
 - personální bezpečnost
 - fyzická bezpečnost a bezpečnost prostředí
 - řízení provozu a komunikací
 - řízení přístupu
 - vývoj a údržba systémů
 - řízení kontinuity operací
 - soulad s požadavky
- automatizovaný nástroj CRAMM

Certifikace

- potvrzení absolvování evaluace, shoda s normou

Co je to hrozba?

- skutečnost, která může způsobit bezp. incident
- přerušení
- zachycení
- modifikace
- fabrikace
- bezpečnostní incident = naplnění hrozby
- dopad = finanční vyjádření bezp. incidentu
- míra rizika = rozsah hrozeb a jejich pravděpodobnost

Common criteria

- metanorma, principy a postupy pro technické normy
- akreditované zkušební laboratoře
- proces vyhodnocování:
 - evaluační kritéria
 - evaluační metodologie
 - evaluační schéma
 - evaluace
 - výsledky evaluace
 - certifikace
 - registr certifikátů
- funkční třídy
- jistotní třídy

- vyhodnocení kvality bezp. mechanismu
- úrovně vyhodnocení dle kritérií

Dvou-třířázový update

- 2 – záměr, zápis
- 3 – záměr, quorum, zápis

Dynamické metody testování

- funkční testování
- analýza mezních hodnot
- testování rozhraní
- testování výkonu

Evaluace

- IS podroben sérii testů
- Common Evaluation Methodology

Granularita oprávnění

- kontrola přístupu na různých úrovních
- režie kontroly vs. dostatečně jemné rozlišení
- byte
- věta
- soubor
- adresář

Granularita autorizace

- ochrana po skupinách
- hesla a jiné tokeny
- dočasné propůjčení oprávnění
- VAX VMS/SE
- systém rolí a skupin

Hesla

- znaky
- délka
- neobvyklé slovo/fráze
- nepravděpodobné
- často obměňované
- nikde poznamenané
- alternativa: passphrase
- skupinová hesla
- PIN

Challenge-Response systémy

- výzva náhodnou zprávou

Chráněné objekty OS

- paměť
- procesor
- spustitelné programy
- sdílená zařízení
- sériově znovupoužitelná zařízení
- sdílená data

Identifikace hodnot (aktiv)

- určení hodnot komponent systému
- hardware
- software
- data
- lidé
- dokumentace
- spotřební materiál

Integrita dat při přenosu

- kryptografické kontrolní součty
- pořadová čísla
- ověřování zpráv centrální autoritou

Integrita databáze

- integrita databáze
- elementární integrita
- elementární správnost

ITSEC

- Information Technology Security Evaluation Criteria
- mezinárodní sada kritérií, nadmnožina TCSEC
- třídy funkčnosti (F)
 - integrita systému (F-IN)
 - dostupnost systémových zdrojů (F-AV)
 - integrita dat při komunikaci (F-DI)
 - utajení komunikace (F-DC)
 - bezpečnost v rámci celé sítě (F-DX)
- třídy korektnosti (E) – zvýšení důvěryhodnosti systému
 - E1 – testování
 - E2 – kontrola konfigurace a distribuce
 - E3 – ověření detailního návrhu a zdrojového kódu
 - E4 – zevrubná analýza slabin systému
 - E5 – důkaz, že implementace odpovídá skutečnému návrhu
 - E6 – formální modely a popisy

Jak uchovávat autorizace

- adresář (directory)
- seznam oprávnění (Access Control List)
- přístupová matice (Access Control Matrix)
- způsobilost (Capability)
- Security Labeling
- procedurálně orientovaný přístup

Jednorázové heslo

- konstatní funkce místo konstatní fráze,
- náhodně zvolené vstupní parametry

Kupujete IS na senzitivní informace

- BS7799 – organizační norma
- TCSEC – první ucelená technická norma
- ITSEC – mezinárodní sada kritérií
- Common Criteria

Metody kontroly vstupu (elementární integrita)

- field checks
- kontrola přístupu
- log změn
- kontrola čtyř očí

Metody útoku po síti

- odposlech sítě
- playback starších zpráv
- narušení služeb
- vkládání poškozených zpráv

Model pro komerční organizace

- Clark-Wilson model
- přejímá postupy běžné v účetnictví
- dobře formované transakce
- separace operací
- požadavky vynucení (E) a korektnosti (C)

Očekávaná ztráta

- riziko vztažené k určitému časovému období

Odhad aktiv

- viz. identifikace hodnot

Odhad rizik

- zlepšení obecného povědomí
- identifikace hodnot, slabin a možných kontrol systému
- zlepšení východiska pro strategická rozhodnutí
- lepší rozložení výdajů na bezpečnost
- provedení odhadu rizik
 - identifikace hodnot
 - určení slabin
 - odhad pravděpodobnosti zneužití

- výpočet očekávaných ročních ztrát
- přehled použitelných ochranných mechanismů
- nástin ročních úspor ze zavedení ochranných mechanismů

Ochrana objektů OS

- fyzická separace
- časová separace
- logická separace
- kryptografická separace

Ochrana paměti

- ohrada (fence)
- reloace
- base/bound registry
- značkováná (tagged) architektura
- segmentace
- stránkování

Ochrana perimetru sítě

- firewall
- vstup jen přes otevřené brány
- detekce a prevence narušení
- monitorování a filtrování provozu dovnitř a ven

Ochrana procesoru

- privilegované instrukce
- úrovně oprávnění procesu – procesy rozděleny do tříd
- správa procesorového času
- správa využívání systémových prostředků
- přerušení při nepovolené operaci

Ochrana prostoru (princip plotu)

- stráž
- elektronická ochrana
 - dveřní a okenní kontakty
 - otřesové hlásiče
 - vodičové desky, drátěnné sítě
 - kontaktní matice
 - mikrovlnné, ultrazvukové, infračervené detektory
 - zvukové hlásiče
 - kyvadlové hlásiče
 - průmyslová televize + záznam

Ochrana proti elektromagnetickému vyzařování

- vzdálenost
- zmatení
- speciální vybavení
- vhodné umístění

Personální politika

- pravidla vztahů organizace a zaměstnanců
- důraz na důvěryhodnost zaměstnanců

PKCS

- Public Key Cryptography Standards
- vytvářeny v laboratořích firmy RSA Security
- soubor technických norem popisující implementaci různých nástrojů asymetrické kryptografie
- návody k průmyslové implementaci
- PKCS #7 – formát šifrovaných zpráv
- PKCS #10 – formát žádosti o certifikát
- PKCS #12 – formát certifikátů a privátních klíčů

Problém odvoditelnosti

- odvození senzitivní informace ze znalosti nesenzitivních
- metody
 - přímý útok
 - nepřímý útok
 - součet
 - počet

- medián
- tracker attack
- ochrana
 - rozbor dotazů i s ohledem na minulost
 - ochrana vlastních dat
 - potlačení
 - skrytí

Průnik do OS

- I/O zařízení
- nevyužívání bezpečnostních prostředků procesorů
- kompromis izolace uživatelů vs. sdílení dat
- kontrola oprávněnosti jen jednou
- snaha o obecnost systému

Rozdíl hrozba vs. riziko

- hrozba – existuje nezávisle na opatřeních
- riziko – pravděpodobnost naplnění hrozby

Senzitivita informací

- přirozeně senzitivní
- ze senzitivního zdroje
- deklarované jako senzitivní
- senzitivní atribut nebo záznam
- senzitivní ve vztahu k dříve vyzařeným skutečnostem

Šifrování komunikace

- zašifrování, dešifrování
- kryptosystém
- otevřený text, šifrovaný text
- šifrování na úrovni linky, end-to-end šifrování
- mechanismus distribuce a správy klíčů
- centrální autority

Spojení dvou sítí

- gateway
- filtrování datového toku
- spojení sítí přes veřejné komunikační sítě (VPN)

Spolehlivá síťová komunikace

- spolehlivé síťové rozhraní
 - zajištění před útoky zvenčí
 - bezpečnostní klasifikace dat
 - verifikace oprávněnosti žadatele
 - ověření konzistence došlých dat
 - zamezení míchání dat různého stupně utajení
 - bezpečnost dat nesmí záviset na bezpečnosti linky
- bezpečná komunikace
- bezpečné síťové spojení
 - moduly se vstupními a výstupními sokety

Spolehlivý front-end

- viz. Víceúrovňová bezpečnost v databázích

Správa verzí (konfigurací)

- zajištění integrity programů a dokumentace
- vyhodnocování a zaznamenávání změn
- prevence proti úmyslným změnám
- zabránění nechtěným ztrátám předchozích verzí
- odstranění komplikací při vývoji podobných verzí
- kontrolované sdílení modulů

Srovnání jedno- a víceúrovňových modelů

- viz. Bezpečnostní modely obecně

Statické metody testování

- analýza algoritmů
- čtení kódu
- rozhodovací tabulky
- analýza rozhraní

TCSEC

- Trusted Computer Security Evaluation Criteria
- Orange Book
- třída D – žádná ochrana
- třída C – optional protection
 - C1 – volná ochrana
 - C2 – kontrolovaný přístup
- třída B – mandatory protection
 - B1 – značkováná ochrana
 - B2 – strukturovaná ochrana
 - B3 – bezpečnostní domény
- A1 – verifikovaný návrh

Testy – životní cyklus

- validace požadavků na software
- verifikace a validace návrhu
- verifikace a validace kódu
- testování
- verifikace a validace při používání programu

Tokeny a autentizace

- pouze s pamětí
- tokeny s heslem
- tokeny s logikou
- inteligentní tokeny – smart cards

Úrovně ochrany objektu

- viz. Autorizace a Granularita

Útoky prostřednictvím programů

- trapdoors
- trojský kůň
- salámový útok – zaokrouhlovací chyby
- skryté kanály
- hladové programy
- viry
- červi
- logická bomba

Vícefaktorová autentizace

- několik bezpečnostních mechanismů paralelně
- aktivace silnějšího mechanismu slabším

Víceúrovňová bezpečnost obecně

Víceúrovňová bezpečnost v sítích

- TCB (Trusted Computing Base)

Víceúrovňová bezpečnost v databázích

- parcelizace (partitioning) - subdatabáze
- šifrování – chosen plaintext attack
- integrity lock – klasifikace, checksum
- spolehlivý front-end
- komutativní filtr
- pohled (view)

Víceúrovňové modely

- military security model – neklasifikováno, důvěrné, tajné, přísně tajné + rozdělení do oblastí

- svazový model (lattice model) – obecnější military
- Bell-LaPadula model
- Biba model
- Clark-Wilson model
- Chinese wall model
 - na začátku všechna práva
 - zákaz přístupu k datům ve stejné skupině
- Graham-Denning model – subjekty, objekty, práva a přístupová matice
- Take-Grant systém

Vlastnosti bezpečného OS

- proces vývoje bezpečného OS
 - bezpečnostní modely
 - návrh
 - ověřování
 - implementace
- činnosti OS
 - autentizace uživatelů
 - ochrana paměti
 - řízení přístupu k souborům a I/O
 - alokace a řízení přístupu k obecným objektům
 - zabezpečení sdílení
 - zajištění spravedlivého přístupu
 - meziprocesová komunikace a synchronizace
- principy
 - nejmenší práva
 - ekonomický návrh
 - otevřený návrh
 - úplné zprostředkování
 - povolování operace
 - rozdělení oprávnění
 - nejmenší sdílené prostředky
 - snadná použitelnost

Výběr dat ze statistické databáze

- potlačení malých výsledků
- kombinování výsledků
- modifikace výsledků
- náhodný šum
- náhodný výběr
- náhodné zmatení

Zálohování

- clusterování, on-line, off-line
- obnova – přípravná část, reakce

Zbytkové riziko

- riziko i přes zavedená bezp. opatření

Zotavení po havárii

- plán pro případ poruchy
- cold site
- hot site

Způsobilost (capability)

- nefalšovatelný token
- vlastnictví dává práva vlastníkov