Ochrana

Základní pojmy

- Hrozba - hrozby tj. skutečnosti, které potenciálně mohou být původci bezpečnostního incidentu
- Riziko - rozsah hrozeb spolu s pravděpodobností jejich realizace udává celkovou míru rizika
- Expozice - místo potenciálního útoku / slabina
- Očekávaná ztráta - riziko vztažené k určitému období
- Zbytkové riziko (ideální stav) - Cílem najít místo, kde se bezpečnostní opatření přestávají vyplácet. Nevyloučili jsme zcela riziko incidentu – zbylo zbytkové riziko

Politika

není pravda

- že bezpečnostní politika je jen „pro ty velké“
- že bezpečnostní politika je obrovské množství práce na celé měsíce
- že by bezpečnostní politika nic neřešila
- že vaše bezpečnostní politika musí být zcela jedinečná a šitá od počátku na vás

Bezpečnostní politika
vyjadřuje vůli pracovat na dosažení jistého stupně bezpečnosti bývá rozdělena do více dokumentů

- kdo má zodpovědnost za udržení bezpečnosti - pověřený pracovník, vedení, všichni
- závazky organizace na udržení bezpečnosti - počet vyčleněných pracovníků, minimální výdaje do této oblasti

Důležitější než rozsah - pokrývat všechny důležité okruhy problémů formou, která je srozumitelná všem, kterých se týká.

Politika umožní:

- umožní rozmyslet si, kde vás bota tlačí
- materiál by neměl popisovat neexistující systém - mít je aktuální a “tailor made”
- organizace pohybující se ve stejné branži budou mít podobné nároky na bezpečnost (take inspiration)

Provozování systému:

Provozování systému pro správu informací je spojeno s jistým rizikem (chyba zařízení, obsluhy, programu, vandalismus, krádež, …)

provedení kvalifikovaného odhadu rizik přináší:

- zlepšení obecného povědomí
- identifikace hodnot, slabin a možných kontrol celého systému
- zlepšení východiska pro strategická rozhodnutí

- lepší rozložení výdajů na bezpečnost - některé velmi drahé ochranné mechanismy poskytují pouze malé zvýšení bezpečnosti a popřípadě i naopak

životní cyklus bezpečnostní politiky bezpečnost je proces - bez soustavného přizpůsobování se změnám vnějšího prostředí a vývoji vlastního IS je to celé k ničemu

Najít cíle se zdůvodněním:

- stanovení důležitosti
- maximální výpadek
- maximální ztráta při obnově
- dostupnost
- míra odolnosti vůči útoku
- ...
- odvolávky na normy, zákony, smlouvy

Identifikace a odhad aktiv (inventarizace)

- co vlastně ve svém informačním systému mám a k čemu je to dobré

Přesnější výsledek docílíme sčítáním po jednotlivých kategoriích, např

- hardware - počítače, monitory, pásky, tiskárny, disky, komunikační media, ...
- software - operační systém, koupené programy, vlastní zdrojové kódy, knihovny o data - vlastní uložená data, logy, archivní kopie, listingy, ...
- lidé - pracovníci potřební k správnému chodu sy stému, správci, programátoři o dokumentace - programů, technického vybavení, systému, administrativní postupy
- spotřební materiál - papír, diskety, tonery, pásky do tiskáren, ...
- zákazníci
- image společnosti
- a hlavně, co to PŘINÁŠÍ, což se nejlépe odhadne tak, že prozkoumáte, co se

Vytipování hrozeb

je potřeba určit, co nás bude stát realizovaný bezpečnostní incident

zkoumáte:

- co by se mohlo stát
- kolik vás bude stát náprava (nové pořízení)
- kolik přijdeme (tj. kolik nevyděláme)

... za kolik si pořídíte novou dobrou pověst seriózní firmy s dlouholetou tradicí ... kolik bude stát, když konkurence získá váš tajný návod na výrobu té nejlepší slivovice...

Příklady hrozeb:

- dopad přírodních katastrof - požár, vichřice, záplavy, výpadky napájení, selhání techniky
- poškození třetími osobami - přístupy po síti, vytáčená spojení, hackeři, kolem-jdoucí, lidé zkoumající odpad firmy o následky zlomyslných pracovníků - zklamaní pracovníci, úplatkářství, zvědavci
- důsledky neúmyslných chyb - zadání špatných příkazů, vadných dat, skartace špatných dokumentů, kompromitace tajných materiálů

- … a asi tisíc dalších

Odhad pravděpodobnosti zneužití

- Odhad pomocí četnosti/pravděpodobnosti
- Odhad na základě obecných dat - např. data od pojišťovny, přehled o životnosti a počtu selhání zařízení
- Odhad na základě vlastních dat - za dobu činnosti firmy vzniklé záznamy o závadách zařízení, počtech vadných loginů, …
- Bodovací systém počtu výskytů události – např. dle tabulky
- Delfská metoda - okruh hodnotitelů provede hodnocení dané veličiny + debata

Výpočet očekávaných ročních ztrát

Stačí prostě vynásobit odpovídající dopady a pravděpodobnosti a vše sečíst
nadhodnocení dopadů a četností může vést ke zcela nesmyslným odhadům ztrát
kvalifikovaný odhad ztrát bývá často vyšší, než se obvykle předpokládá

Postprocessing

třeba najít / zodpovědět:

- Jaké právní normy chrání utajení a integritu dat?
- Jaké další normy je nezbytné dodržet?
- Co nás bude stát, pokud se na shora uvedené skutečnosti nebudeme brát ohled.

Návrh řešení

Výsledkem je seznam navrhovaných opatření.

Verifikace / Nástin ročních úspor ze zavedení ochranných mechanismů

S bezpečností je jeden problém – nic užitečného to nedělá
spočítat odhad očekávaných ztrát v aktuálním stavu
známe cenu zavedení nových ochranných mechanismů znovu vyčíslíme očekávanou ztrátu po zavedení těchto opatření
rozdíl těchto hodnot je odhad celkových úspor

Struktura bezpečnostního plánu

bezpečnostní plán popisuje, jak daná organizace přistupuje k otázkám bezpečnosti plán musí být dostatečně často revidován a musí být zkoumáno jeho dodržování vypracováním plánu bývá pověřena skupina odborníků pokud možno ze všech důležitých organizačních struktur firmy, velikost a struktura tohoto týmu závisí na velikosti firmy

součásti bezpečnostního plánu:

Pokrytí

přesný popis, jakými oblastmi IS se zabývá, jaké hrozby uvažuje

Bezpečnostní politika
vyjadřuje vůli pracovat na dosažení jistého stupně bezpečnosti bývá rozdělena do více dokumentů

- kdo má zodpovědnost za udržení bezpečnosti - pověřený pracovník, vedení, všichni
- závazky organizace na udržení bezpečnosti - počet vyčleněných pracovníků, minimální výdaje do této oblasti

Klasifikace hodnot

popis obsahuje seznam hodnot systému, soupis hrozeb pro tyto hodnoty a používané ochranné mechanismy
dále je popsán způsob získávání a vstupní validace dat, případně předpoklady o jejich vlastnostech
měly by být popsány metody odhalování slabin systému, popisy akcí, které je třeba podniknout v případě odhalení nové slabiny odhady ztrát a dopadů vlastníci

Analýza rizik

obecný pohled na situaci
detailní popis relevantních nezanedbatelných rizik

Doporučení

seznam dalších bezpečnostních opatření, které je třeba přijmout k doplnění, nebo nahrazení sočasných mechanismů
součástí by měl být rozbor nákladů a ztrát
seznam by měl být seřazen podle naléhavosti navrhovaných opatření, navrhována by měla být pouze opatření, jejichž celkový efekt není záporný

Odpovědnost za implementaci

je třeba určit konkrétní osoby zodpovědné za zavedení a provozování konkrétních bezpečnostních mechanismů

Soustavná pozornost

je třeba již v plánu stanovit termín, kdy musí být provedeno nové zhodnocení bezpečnostní situace a ověření funkčnosti bezpečnostních aktivit
získaná ocenění hodnot a bezpečnostních rizik musí být průběžně aktualizována

Závazek dodržování bezpečnostního plánu

všichni pracovníci by měli být s bezpečnostním plánem seznámeni a měla by jim být vysvětlena jeho důležitost i jejich role v rámci plánu
podstatné je, aby vedení organizace přijalo závazek, že bude poskytovat dostatečnou podporu provádění bezpečnostního plánu

---

Bezpečnost

Hlavní komponenty bezpečnosti lze rozdělit takto:

- kontrola prostředí

- autentizace / identita
- autorizace
- separace
  - fyzická
  - časová
  - logická
  - kryptografická
- integrita
- dostupnost
- auditabilita

zde se naplánuje,

- jak budete řešit všechny oblasti bezpečnosti,
- kdo je za co zodpovědný a
- jak to budete implementovat a provozovat.

Realizace a provoz

realizace, provoz, monitorování, aplikace změn, verifikace, audit, ...

možné hrozby

- přerušení - některá část systému je ztracena nebo nedosažitelná
- zachycení - neautorizovaný subjekt získá přístup k nějakému objektu systému
- modifikace - neautorizovaný subjekt získá možnost pozměňovat některé části systému
- fabrikace - neautorizované vytvoření nového objektu
- ...
- obecně narušení některé z požadovaných vlastností systému

zdroje ohrožení

- přírodní (vyšší moc)
- závady hw
- neúmyslné lidské chyby
- záměrné útoky

klasifikace útočníků

- I. způsobu, jak se projeví způsobená škoda
  - A. ztráta integrity
  - B. ztráta dosažitelnosti
  - C. ztráta autenticity ...
- II. druhu způsobené ztráty
  - A. neautorizované použití služeb
  - B. přímá finanční ztráta
  - C. fyzické poškození, vandalismus
- III. role, kterou výpočetní technika hraje v tomto konání
  - A. objekt útoku
  - B. nástroj

    - C. prostředí
    - D. symbol
- IV. použitých prostředků
    - A. opisování údajů
    - B. špionáž
    - C. vkládání falešných dat
    - D. krádež
    - E. odposlech
    - F. scanování, prohledávání - kupříkladu hledání hesel zkoušením, hledání tfn. linek, které vedou k počítači, ...
    - G. piggybacking, tailgating - útočník se snaží projít vstupní kontrolou zároveň s autorizavanou osobou, nebo pokračovat v započaté session H. trojské koně - programy, vykonávající skrytou funkci
    - I. viry
    - J. trapdoors - skryté vstupy do systému, utajené příkazy umožňující přeskočit některé části procesu
    - K. logické bomby - části kódu spouštěné výskytem určitých okolností - čas, dosažený obrat, stav systému
    - L. salami attack - využívání zaokrouhlovacích chyb, drobné úpravy na hranici přesnosti zpracovávaných dat
    - M. prosakování dat
    - N. pirátství

Normy

potřebujeme normy pro jednotná kritéria, abychom na nic nezapomněli, usnadňují audity

- formální verifikace - bezpečnost převedena na soustavu logických formulí
- validace - obecnější metoda
    - testování požadavků - testuje, zda je splněn každý z požadavků na funkčnost systému
    - kontroly návrhu a kódu
    - testování modulů a celého systému - na zkušebních datech
- tiger team penetration team - třetí strana pověřená proniknout bezpečnostními mechanismy

pokud systém obstojí při validaci, může mu být vystaven certifikát, který je formálním vyjádřením s požadavky příslušné normy

Zdroje požadavků na bezpečnost

- zákony
- oborové normy/standardy
- vnitrofiremní směrnice
- požadavky obchodních partnerů

Orange book / TCSEC

- tvůrcem je ministry of defense US
- první ucelená technická norma

Čtyři základní třídy:

- D - žádná ochrana
- C - optional protection - musí být k dispozici příslušný mechanismus, který uživatel může použít
  - C1 - volná ochrana - oddělení uživatelů od dat
  - C2 - kontrolovaný přístup
    - každý uživatel oddělen
    - rezidua (obsah paměti, registrů) poté, co je systém přestane používat, nesmí být zpřístupněna
    - musí být vede access log
- B - mandatory protection - musí být k dispozici odpovídající mechanismus, který uživatel nemůže obejít ani deaktivovat
  - B1 - značkovaná ochrana
    - každý subjekt má stupeň utajení
    - každý přístup dle Bell-LaPadula modelu
  - B2 - strukturovaná ochrana
    - verifikovaný globální návrh systému
    - rozdělení do nezávislých modulů
    - nejmenší možná oprávnění
    - analýza možných skrytých kanálů
  - B3 - bezpečnostní domény
    - podrobení extenzivnímu testování
    - úplný popis celkové struktury návrhu systému
    - koncepčně jednoduchý
    - kontrola na úrovni provádění jednotlivých typů přístupu
- A1
  - návrh systému je formálně verifikován
    - existuje formální model s důkazem konzistentnosti, ověřením, že odpovídá danému systému, že implementace je shodná se specifikací
  - formální analýza skrytých kanálů

ITSEC

- nadmnožina TCSEC
- kritéria rozdělena do funkčnosti (F) a korektnosti (E)
- třídy funkčnosti cca odpovídají TCSEC (C1-B3)
- funkčnost hodnocena v
  - integritě systému (F-IN)
  - dostupnosti systémových zdrojů (F-AV)
  - integritě dat při komunikaci (F-DI)
  - utajení komunikace (F-DC)
  - bezpečnosti v rámci celé sítě (F-DX)
- každá nezávisle na ostatních
- korektnost (C2 - A1 v TCSEC)
  - E1 - testování
  - E2 - kontrola konfigurace a distribuce
  - E3 - ověření návrhu a kódu
  - E4 - analýza slabin systému
  - E5 - důkaz, že implementace odpovídá specifikaci
  - E6 - formální modely (formální popis a vzájemná korepondence)

Common criteria

- metanorma stanovující princip a postup jak odvozovat technické normy pro vývoj, testování a provoz
- evaluační kritéria -> evaluační metodologie -> evaluační schéma -> evaluace -> výsledky -> certifikace -> registr certifikátů
- oddělení functional requirements od assurance
- functional třídy
  - FAU – bezpečnostní audit
  - FCO – komunikace
  - FCS – kryptografická podpora
  - FDP – ochrana uživ. dat
  - FIA – identifikace a autentizace
  - FMT – bezpečnostní management
  - FPR – soukromí
  - FSP – ochrana bezp. mechanismu
  - FRU – využívání prostředků
  - FTA – přístup
  - FTP – důvěryhodná cesta/kanál
- assurance třídy
  - ACM – správa konfigurací
  - ADO – dodávka a provoz
  - ADV – vývoj
  - AGD – dokumentace, návody
  - ALC – podpora životního cyklu
  - ATE – testování
  - AVA – vyhodnocení slabin
- vyhodnocení kvality bezpečnostního mechanismu
  - APE – vyhodnocení profilu bezpečnosti
  - ASE – vyhodnocení cíle hodnocení
- assurance level
  - EAL1 – funkční testování
  - EAL2 – strukturální testování
  - EAL3 – metodické testování a kontroly
  - EAL4 – metodický návrh, testování a ověření
  - EAL5 – semiformální návrh a testování
  - EAL6 – semiformálně verifikovaný návrh a testování
  - EAL7 – formální návrh a testování

ISO 17999 / BS7799

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

- popisuje jaké činnosti musí organizace vykonávat pro bezpečnost IS
  X
- nespecifikuje přímo kvalitu
- bezpečnost shora dolů (politika -> implementace)
- pro lehci implementaci BS7799 - existuje standardní metodika a automatizovaný nástroj CRAMM

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 (právní, technické, audit)

Standardy PKCS

- ucelený soubor technických norem popisující impementaci nástrojů asymetrické kryprografie
- v laboratořích RSA Security
- původně proprietární normy, dnes široce používaný de-facto standard

Modely

první fází tvorby bezpečného IS je volba vhodného bezpečnostního modelu připomeňme dodržení základních požadavků bezpečnosti:

- utajení,
- integrita,
- dostupnost,
- anonymita, …
  dále budeme předpokládat, že umíme rozhodnout, zda danému subjektu poskytnout přístup k požadovanému objektu, modely poskytují pouze mechanismus pro rozhodování

Jednoúrovňové

Monitor model

též reference monitor
• subjekt při přístupu k objektu vyvolá tzv. monitor a předá mu žádost jakou akci s kterým objektem chce provést
• monitor žádost vyhodnotí a na základě informací o přístupových právech vyhoví či nikoliv

výhodou jednoduchost a snadná implementovatelnost
nevýhodou je, že proces poskytující služby monitoruje volán při každém přístupu k libovolnému objektu, což systém velmi zatěžuje
další nevýhodou je, že tento model je schopen kontrolovat pouze přímé přístupy k datům, ale není schopen zachytit např. následující případ

```
1  if profit <= 0
2  then
3    delete file F
4  else
5    write file F,
6    “_zpráva_”
7  endif
```

subjekt mající legitimní přístup k souboru F může získávat informace o proměnné profit, k níž by přístup mít neměl

Information flow model

odstraňuje posledně jmenovanou nevýhodu předchozího modelu
autoři si všimli, že uživatel může získávat i jiné informace, než na které se explicitně ptá
již ve fázi vývoje je prováděno testování všech modulů, zda jejich výstupy závisí na interakcích se senzitivními daty a případně jakým způsobem
z těchto dílčích výsledků je sestavován celkový graf závilostí
veškeré požadavky na systém procházejí inteligentním filtrem, který zjišťuje, zda nedochází k nežádoucí kompromitaci informací

Modely pro specifické účely

Clark-Wilson model

pravidla modelu rozdělujeme obvykle na požadavky na korektnost „C“ a na vynucení „E“
C1 – Všechny procedury testující validitu dat musí zajistit, že pokud doběhnou, všechna chráněná data jsou korektní.
C2 – Všechny používané transformační procedury musí být certifikovány, že po zpracování korektních chráněných dat zanechají chráněná data opět v korektním stavu.
E1 – Systém musí zajistit, že pouze procedury vyhovující požadavku C2 mohou pracovat s chráněnými objekty.
E2 – Systém musí udržovat seznam relací popisující, který subjekt smí spouštět které transformační procedury a musí zajistit dodržování těchto relací.
C3 – Seznam popsaný v E2 musí splňovat pravidlo separace odpovědností.
E3 – Systém musí autentizovat každý subjekt pokoušející se spustit transformační proceduru.
C4 – Všechny transformační procedury musí zapisovat do append-only objektu (log) veškeré informace nezbytné pro rekonstrukci povahy provedené operace.
C5 – Každá transformační procedura zpracovávající nechráněná data musí buď skončit s tím, že chráněná data jsou v korektním stavu, nebo nesmí provést žádnou změnu.
E4 – Pouze administrátor provádějící certifikaci entit může provádět změny relací. V žádném případě nesmí mít právo spustit žádnou z procedur, které administruje.

Chinese wall model (Brewer-Nash)

Dynamický model – pravidla jsou generována až v okamžiku používání řízených objektů

„Konzultant musí zachovávat diskrétnost informací získaných v různých firmách, tj. nesmí radit konkurenční firmě na základě vnitřních znalostí jiné korporace. Může ale radit nekonkurenčním firmám, případně může dávat rady na základě obecných informací“.

objekty jedné organizace tvoří dataset, datasety rozčleněny do tříd (conflict of interest classes)

sanitizovana informace - odstranene casti umoznujici identifikaci vlastnika

subjekt na počátku univerzální práva (ke všem objektům)

Vlastnost jednoduché bezpečnosti
Přístup je povolen pokud požadovaný objekt:

1. je ve stejném datasetu jako objekt, ke kterému subjekt již přistupoval, nebo
2. náleží do jiné třídy

*-vlastnost
Zápis je povolen pouze v případě že:

1. přístup je možný podle vlastnosti jednoduché bezpečnosti, a zároveň
2. není čten žádný objekt obsahující nesanitizované informace náležející do jiného datasetu než toho, do kterého se zapisuje

Graham-Denning model

model pracuje s množinou subjektů S, množinou objektů O, množinou práv R a přístupovou maticí A.

- vytvořit objekt o
- vytvořit subjekt s
- zrušit objekt o vlastník je v A[x,o]
- zrušit subjekt s vlastník je v A[x,s]
- číst přístupová práva s k o kontroler je v A[x,s], nebo vlastník v A[x,o]
- zrušit přístupové právo r subjektu s k o kontroler je v A[x,s], nebo vlastník v A[x,o]
- přidělit s právo r k objektu o vlastník je v A[x,o]
- předat přístupové právo r nebo r* k objektu o subjektu s r* je v A[x,o] r* označuje předatel

Take-Grant system

model pracuje s čtyřmi základními primitivami: create, revoke, take, grant.

předpokládáme, že systému obsahuje množinu subjektů S, množinu objektů O, objekty dělíme na aktivní (zároveň i subjekty) a pasivní (nejsou subjekty) a množinu práv R

Výhodou popsaného systému je, že umožňuje v subpolynomiálním čase řešit dotazy na dostupnost jistého objektu pro daný subjekt

Víceúrovňové

Military security model

KVP (stupeň utajení, oblast) - smím ze nějakého stroje s nějakým loginem přistoupit k těm a těm datům?

Svazový model

Částečné uspořádáním

Bell-LaPadula model

model popisuje povolené přesuny informací, takové, aby bylo zajištěno jejich utajení
pro každý subjekt S resp. objekt O v systému nechť je definována bezpečnostní třída C(S) resp. C(O)
bezpečné přesuny informací mají následující vlastnoti:
Vlastnost jednoduché bezpečnosti (Simple Security Property):
Subjekt S může číst objekt O právě když
C(O)≤ C(S).

-*vlastnost (*-Property):
Subjekt S mající právo čtení k objektu O může zapisovat do objektu P právě když
C(O)≤ C§.

Biba model

předchozí model se však vůbec nezabývá integritou dat, Biba model je duálním modelem k Bell-LaPadula modelu
Nechť pro každý subjekt S resp. objekt O v systému je definována integritní bezpečnostní třída I(S) resp. I(O).
Obdobně jako v předchozím případě definujeme:
Vlastnost jednoduché integrity (Simple Integrity Property):
Subjekt S může modifikovat objekt O právě když
I(O)≤ I(S).

Integritní *-vlastnost (Integrity *-Property):
Subjekt S mající právo čtení k objektu O může zapisovat do objektu P právě když
I(O)≥ I§.

Biba model se zabývá zajištěním integrity a tedy i důvěryhodnosti dat. Bepečnostní třída entity vpodstatě popisuje míru její důvěryhodnosti pro ostatní.
Tento model vůbec neřeší utajení dat.

Přestože byla učiněna řada pokusů o nalezení kompromisu mezi zajištěním integrity a utajení, dosud neexistuje obecně přijatý model, který by řešil oba problémy.

Autentizace

- zjištění/ověření identity subjektu
- identifikátory: jméno, userID, rodné číslo, …
- primární identifikující dokumenty: op, pas, úřední dokumenty s fotkou
- sekundární identifikující dokumenty: směnka, výplatní páska, …
- identifikující charakteristika: biometrika, fotografie
- entita: bytost, místo, věc

registrace

- iniciální přiřzení identifikačních dokumentů entitě

identita uživatele

- struktura označovaná jako profil
- userID, heslo
- jméno, příjmení, tituly
- certifikáty, klíče
- oprávnění

pojmy: alias, anonymita, pseudonymita

autentizace protistrany

- co ví pouze dotyčná osoba
  - heslo, pass-phrase, šifrovací klíč
- co vlastní
  - token, schopnost, znalost
- schopnost provést operaci
  - cosi charakteristického
  - biometrika

heslo

- není omezeno jen např. na malá písmena a čísla
- dostatečná délka
- není známou frází
- nepravděpodobné, nelze odvodit ze znalosti osoby vlastníka
- často obměňované
- není po okolí poznamenané
- passphrase
  - velmi dlouhá hesla, třeba citát z knihy

skupinová hesla

- zná celá skupina
- bývají často vyzrazena

PIN

- číselné řetězce standardní délky

Challenge-response systémy

- heslo zachyceno v průběhu vkládání
- např. systém zašle náhodnou zprávu a uživatel ji zašifruje klíčem a pošle zpět

jednorázová hesla

vícefaktorová autentizace

- kombinace několika autentizačních postupů
- několik nezávislých mechanismů aplikovaných paralelně, nebo sériově

výměna taností

- protokol pro případ, že komunikující strany nedůvěřují okolí a nechtějí vyzrazovat identitu
- pokud sdílejí/nesdílejí tajný klíč
- TODO:

asymetrické klíče

- ověřovatel zašle dokazovanému náhodně volený řetězec
- dokazovaný jej transformuje za použití soukromého klíče
- ověřovatel pomocí veřejného klíče ověří správnost

symetrické klíče

- podobný princip

passphrases

- dlouhá hesla, součást písní, básniček
- lehce zapamatovatelná
- lze aplikovat další měření (např. rytmus stisku kláves bývá charakteristický)

tokeny, smart cards

- token je předmět, který autentizuje svého vlastníka
- musí být jedinečný a nepadělatelný
- magnetické/čipové karty
- pokud má vlastní výpočetní kapacitu, pak smart card
- pouze s pamětí
  - obdoba mechanických klíčů
- udržující hesla
  - po zadání hesla vydá určený kvalitní klíč, který udržuje
- s logikou
  - umí zpracovávat jednoduché podněty, např: vydej následující klíč
  - lze realizovat one time hesla
- smart cards (inteligentní tokeny)
  - mohou např. generovat náhodná čísla
  - lze nimi doplnit challenge-response systémy

biometriky

- identifikace lidí na základě jejich osobních charakteristik
- navzájem různé mírou spolehlivosti, ceny a společenskou přijatelností
- ideální velká mezi-osobní variabilita a dobrá vnitro-osobní reproducibilita
- četnost false negatives
- četnost false positives (útok)

verifikace hlasu

- subjekt přečte systémem náhodně zvolenou frázi
- proveden rozbor zvuku
- snadné využití (i např. pomocí telefonu)

verifikace dynamiky podpisu

- sledují se změny tlaku, zrychlení v čase, celková dráhá, apod…
- výhodou je přirozenout a sociální akceptovatelnost
- nevýhodou je variabilita podpisu u lidí

verifikace otisků prstů

- statistický rozbor výskytu markant (hrboly, smyčky, spirály)
- dobrá mezi-osobní variabilita a vnitro-osobní reproducibilita
- občas sporná spolehlivost snímačů

geometrie ruky

- metoda zkoumá délku a šířku dlaně a jednotlivých prstů, boční profil ruky apod…
- spolehlivá, ale drahá
- možnost podrstření podlitku ruky

obraz sítnice

- zařízení pořídí obraz struktury sítnice v okolí slepé skvrny
- velmi obtížná napodobitelnost
- drahá věc, osobně možná nepříjemné

další biometriky

- rysy obličeje
- otisky chrubu, genetické rozbory

Autorizace

úrovně

- žádná (nebo samovolná časová separace)
- izolace (procesy vůbec o sobě nevědí)
- sdílení všeho nebo ničeho
- sdílení s omezenými přístupy (přístupy jsou spravovány)
- sílení podle způsobeilosti (rozsah může dynamicky záviste na kontextu)
- limitované použití objektu (specifikuje i různé druhy operací, které může přistupovatel vykonávat)

granularita

- kontrola přístupu může být na různých úrovních

objekty ochrany

- systémové zdroje
- data na systému
- datové struktury
- služby

cíle ochrany objektů

- kontrola každého přístupu
- povolení co nejmenších práv
- ověření správného používání
- omezení rozsahu používání

mechanismus ochrany obecných objektů

- rozhodovací algoritmus
- autorizační data

adresář
každý uživatel má práva k nějakému souboru (speciálně vlastník), tato práva jsou popsána v adresáři každého uživatele
žádný uživatel nemá práva na adresář uživatele

seznam oprávnění
každý objekt má vedle sebe seznam informací, které subjekty k němu mají opravnění
lze např používat regexy na označení práv

přístupová matice
řádky jsou subjekty, sloupce objekty, číslo určuje druh práva
velmi řidká a velká

způsobilost
nefalšovatelný token
třeba seznam způsobilostí každého běžícího procesu (v chráněné paměti)

security label
každý subjekt má bezpečnostní label popisující pověření/klasifikaci

procedurálně orientovaný přístup
subjekty mají práva/nepráva k funkcím z rozhrání, prostřednictvím kterého je objekt zpřístupňován
ztráta efektivity, ale podporuje zapouzdřování

granularita autorizace

ochrana po skupinách
každý objekt má práva pro vlastníka, skupinu a okolní svět

hesla a tokeny
při vytvoření vlastník specifkuje hesla potřebná pro jisté módy přístupu
hesla jsou zaslána uživatelům
je náročné udržovat a spravovat hesla (vystavit nové, zinvalidovat subjekt apod...)

dočasné propůjčení oprávnění
stejně jako ochrana po skupinách, ale lze nastavit, zdali se soubor spouští s oprávněním vlastníka
lze tak zprostředkovaně přistupovat k prostředkům, ke kterým původní subjekt nemá právo
o něco náročněji implementovatelné a těžko se spracuje

VAX VMS/SE
každý soubor má seznam oprávnění udávající kdo má jaká práva

systém rolí a skupin
oprávnění jsou sdružována do ucelených souhrnů - rolí, které odpovídají svým obsahem okruhu práce, kterou vykonává pracovník
uživatel nezískává oprávnění “po jednom”, ale přidělením role
lze role stavět hiearchicky pro snazší spravování

referenční uživatelé
předpřipravené vzory častých typů uživatelů
usnadňují správu

Fyzická bezpečnost

snaha eliminovat hrozbu ještě dříve, než přijde do kontaktu se systémem

přírodní katastrofy

celkově je dobré mít označené důležitosti komponent systému pro dobrou strategii
záplavy - stoupající voda, většinou lze v mezičase přesunout alespoň data
požáry - ohrožení i pro personál
ztráta napájení

- je třeba zajistit alternativní zdroje energie, akumulátory a UPS zdroje
- důležité také filtry a přepěťové ochrany před blesky apod
  chlazení - některé komponenty jsou citlivé na teplo
  hmotnost - některá technika vyžaduje podlahy se zvýšenou nosností
  prašnost, vibrace, další vlivy

prostorová ochrana

prostředky zabraňující útočníkům ve vstupu do prostor systémů/výnosu komponent

stráže - musí znát všechny pracovníky, nebo schopna ověřit, třeba tokenem
elektronická prostorová ochrana

- dveřní a okenní kontakty detekují otevření
- otřesové hlásiče, vodičové desky, drátěné sítě - detekují rozbití nebo proražení střežené plochy
- kontaktní matice - instalovány pod podlahu, detekují vstup
- mikrovlnné, ultrazvukové a infračervené detektory - ragují na změnu/přeručení svazku příslušného záření
- zvukové a kyvadlové hlásiče

detekce výstupu - třeba v obchodních domech, komponenty mají tagy/nálepky

likvidace médií se senzitivními informacemi
zkartovače - liší se jemností
přepisování magnetiký médií - lze přepas na nuly, není ale 100% spolehlivé
degaussery - vygenerováním silného elektromagnetického pulzu zničí původní pole, není ale 100% spolehlivé

odpovědnost za zabezpečení

- odpovědnost za návrh bezpečností strategie

- odpovědnost za dodržování návrhu
- důležité jsou opakované namátkové kontroly

elektromagnetické vyzařování

- lze z toho odvodit nějaké informace (monitor, vodiče)
- nelze kriminalizovat
- řešení:
  - vzdálenost
  - zmatení - posílat fuzzy signály
  - speciální vynutí
  - vhodné umístění do stíněných prostor

obnova provozu - dostupnost
účinné zálohování je součást bezpečnostní strategie
agilní zotavení z chyb
archivní kopie různých stádií projektu

zálohy na nejrůznější zařízení
samotné zálohy ve standardním formátu
verifikace vytvořené záložní kopie
komprese a deduplikace ukládání dat (rychlost a menší objem dat)
kryptografická ochrana dat (jinak vulnerable)
snadno specifikovatelné kdy zálohovat
SW pro zálohu musí být opravdu otestován

záložní média
výměnné - usb disky, pásky, worm disky, hard copy
další:
disky (disk mirroring - zápisy na jednom disku jsou automaticky duplikována)
duplexing - dva stroje mají přesně stejný obsah paměti a synchronně provádějí veškeré operace (při výpadku jednoho pokračuje druhý)
síť - zálohování je kopírováním na další počítač v síti (je třeba zajistit bezpečnost a flexibility zotavení)

zálohy hardware

- je nutné mít záložní systém, nebo alespoň kritické nahraditelné součástky

zásady pro pořízování záloh

- závisí na situaci a cejména na objemu dat

ztráta dat - velmi problematická, neboť znovupořízení může být náročné
ztráta software

- je zpravidla možno znovu nainstalovat, ale je nutná opětovná konfigurace
- konfigurační soubory by tedy měly být zálohovány

pokud je místo a čas, je dobré provádět zálohu všech dat a programů
dříve Grandfather-Father-Son, nejnovější vždy přepisoval nejstarší

nyní se však zálohuje jen konkrétní část (databáze, OS, aplikace, ...)
četnost je úměrná důležitosti

důležité milníky záloh by měly být uloženy na bezpečných místech

plány kontinuity

organizace musí mít připravené postupy pro případ haváre po dobu bez

- podpory informačního systému
- vlastního zaškoleného personálu
- komunikace
- provozních prostor ...

plán obnovy - pro případ poruchy je třeba mít vypracované a otestované procedury

obnova provozu

- občas velmi kritické znovu obnovit výpočet
- výrobci většinou rychle dokáží dodat nový systém během dne
- cold site
  - zařízení vybavené zdroji, klimatizací, komunikacemi apod
  - je třeba přinést systém
- hot site
  - už obsahuje systém
  - je třeba jen přinést zálohu dat a programů
- clustery
  - redundance na úrovni funkčních jednotek (serverů, systémů) zajišťující automatické přenesení výpočtu na zbylé kapacity
- mirroring - online redundance na úrovni datových úložišť
- zálohy

RTO recovery time objective RPO recovery point objective

i moc lehce dostupne zalohy jsou blbe - lide potom zkousi blbosti, protoze maji lehky zpusob obnovy

ZVČ: při větším množství zařízení se musí počítat s chybami (např. Google s miliony HDD)

SW

Malitious

trapdoors - nedokumentovaný vstup do prgramového modulu (obvykle debug mód)
trojan horses - program vykonává navíc i zákeřné věci
salami attack - využívá zaokrouhlovacích chyb, těžko detekovatelné

skryté kanály (covert channels)

- výnos informací
- fake chyby ve výpisech

- vznik systémových událostí
- nepatrné změny frontendu

exploits

- známé slabiny programů
- existuje spousta nástrojů pro detekci podmnožiny

proti dosažitelnost služeb systému

hladové programy, DOS útoky

- mohou generovat velké množství synovských procesů
- mohou běžet v nekonečné smyčce
- spousta těžkých IO operací (i síťových)

viry

- malý program s autoreprodukční schopností
- často nahrazuje část jiného programu
- obsahují mechanismy proti detekci
- po určitou dobu vykonávají pouze reprodukci
- prevence je oddělení systémů, aby nemohlo dojít k přenosu

worms

- síťová obdoba virů, mají schopnost se šíři pomocí sítě
- prevence je patřičné rozdělení, používání pouze testovaného sw

metody vývoje

modularita, zapouzdření, ukrytí informací

- rozdělení na nezávislé moduly (microservices? :^))
- pořádně zdokumentované rozhrání

nezávislé testování - nezávislý tým

správa verzí a konfigurací

- zabraňuje úmyslným změnám odzkoušených programů (vkládání trapdoors)
- zabraňuje ztrávtám předchozích verzí software
- odstraňuje komplikace při vývoji více verzí
- mechanismus pro kontrolované sdílení modul (prostě version control)

spolehlivý software

- program je funkčně korektní, pokud vykonává správně všechny očekávané funkce a nic víc
- spolehlivý sw (trusted) jsou programy, které jsou funkčně korektní a vyžadují to i u modulů, které spouštějí
- operační systém by měl být spolehlivý sw

spolehlivé programy

- funkční korektnost
- zajištění integrity - zachová korektnost dat i při špatném vstupu
- omezená práva - pokud má přístup k utajovaným datům, minimalizuje kontakt
- zajišťuje přístup k citlivým datům pro obecně nespolehlivé uživatele, kterým není možné dát přímý přístup

vzájemné podezřívání (mutual suspicion)

- předpokládat, že ostatní programy jsou hloupé
- nevěřit, že předávají korektní vstupy
- komunikace pouze poocí dobře chráněného rozhrání

omezení (confinement)

- podezřelý program má přísně vymezeno, jaké systémoé zdroje smí používat (sandbox)
- Windows *runas*, UNIX *chroot*

parcelizace informací (information comparement)

- veškerá data a programy v systému jsou rozdělena do několika oblastí
- každý program může pracovat s daty z nejvýše jedné oblasti, do které sám patří

access log

- vše logovat (co, kdo, kdy, jak dlouho, s čím)
- zaznamenávat zejména chyby a pokusy o nepovolené přístupy

administrativní nástroje ochrany

není fajn dávat programátorům úplně volnou ruku, neboť kód musí být verifikovatelný, udržovatelný apod
standardní návrh - obvykle seznam povolených vývojových prostředků, jazyků a metodologií
standardy pro tvorbu dokumentace, stylu kódování, pojmenování proměnných apod
standardy programování - programování ve větším měřítku, systém peer reviews, audity
standardy testování - verifikační metody, archivování výsledků testů
standardy konfiguračního managementu - způsoby výměny produktů, zaznamenávání změn apod

dodržování - bez toho nemá smysl

- klíčové momenty tendence porušení pravidel jsou při zpoždění projektu a odchodu klíčových pracovníků

pokud programátor očekává, že neznámý člověk bude testovat jeho kód, snaží se víc

charakter přijímání pracovníků

- podstatné jsou reference z předchozích pracovišť, psychologické testy apod
- až postupně získává důvěru a větší a větší přístup

sledování pracovníků

- dobré mít ponětí o extrémních a finančních aktivitách

Verifikace a validace

cíl je důkladná analýza a testování
provádí se v průběhu a po dokončení díla
nezávisle na vývoji po stránce

- technické - jiní lidé než vývojáři
- řídící - tým si sám volí co testuje
- finanční - tým musí být zodpovědný pouze za testování, nikoliv za funkčnost projektu

řízení v&v

- pareto efekt - 20% chyb spotřebuje 80% nákladů na předělávky
- je dobré mít analýzu hazardů a kritických sekcí

aktivity v&v

- validace požadavků - zdali nejsou v rozporu s platnými standardy, nejsou vnitřně sporné
- v&v návrhu sw - ověřit, že návrh splňuje požadavky
- v&v kódu - ověřit, že kód implementuje návrh
- testování (modulů, integrace, systému, instalace)
- v&v při správě a používání sw

TODO: table

v&v techniky

- statické - přímo zkoumají struktury a formu produktu bez jeho spuštění (reviews, inspekce, data-flow)
- dynamické - analýza výsledků zkušebních běhů a simulací
- formální - matematická analýza
- analýza algoritmů
- analytické modelování
- back-to-back testing
- analýza mezních hodnot
- čtení kódu
- analýza toku řízení
- analýza pokrytí
- kritická analýza
- databázová analýza
- analýza toku dat
- rozhodovací tabulky
- desk checking
- error seeding
- event tree analysis
- konečné automaty
- funkční testování
- inspekce
- analýza rozhraní
- testování rozhraní
- analýza mutací
- testováí výkonu
- petriho sítě

- důkaz korektnosti
- prototypování
- regresní analýza a testy
- procházení požadavků
- reviews
- sensitivity analysis
- simulation
- sizing a analýza časování
- slicing
- chybový mód, efekty, kritická analýza
- analýza chybných stromů
- stress testing
- strukturální testování
- symbolické spouštění
- certifikace testů
- procházky

v&v pro znovupoužitý SW

- analýza konzistence
- analýza rozhraní

specifické pro báze znalostí

- alternativní model
- control groups
- analýza kredibility
- field testing
- testování nepovolených atributů
- logická verifikace
- meta modely
- partition testing
- verifikace pravidel
- statická validace
- turingův test
- weight analysis

Aplikační server

- využívá OS a databázi jako persistentní repository vlastních dat včetně nastavení bezpečnostního mechanismu

OS

chráněné objekty

- procesor
- paměť
- spustitelné programy

- sdílená zařízení typu sidky
- sériově znovupoužitelná zařízení - tiskárny, pásky
- sdílená data

poskytované služby
ochrana procesoru
metody ochrany objektů v operačních systémech

ochrana paměti a adresování

- ohrada (fence)
- relokace
- base/bound registry
- značkovaná (tagged) architektura
- segmentace
- stránkování

ochrana obecných objektů

- seznam
- cíle

autentizace subjektů

- hesla
    - hledání hesel
        - textové soubory
        - zašifrované soubory
        - one time passwords

návrh bezpečných OS

- autentizace uživatelů
- ochrana paměti
- řízení přístupu k souborům a IO
- alokace a řízení přístupu k obecným objektům
- zabezpečení sdílení
- zabezpečení spravedlivého přístupu
- meziprocesorová komunikace a synchronizace

namátkou

- virtuální adresní prostor
- virtual machine
- kernel
- vrstvový model
- kruhová struktura

průniky OS

- TODO

problémy virtualizace

DBs

fyzická integrita
logická integrita
elementární integrita
auditabilita
kontrola přístupu
autentizace uživatelů
dostupnost

integirta

- dvoufázový update
- třífázový update
- redundance/vnitřní konzistance
  - detekční a samoopravné kódy
  - stinné záznamy

zotavení
paralelismus/konzistence
monitory

porovnání mezí
stavová omezení
tranzitivní omezení

senzitivní data
rozhodování o přístupu

- dostupnost dat
- akceptovatelnost přístupu
- zajištění autenticity

vyzrazení dat

- přesné hodnoty
- meze
- negativní výsledek
- existence
- pravděpodobné hodnoty
- součet
- počet
- medián

bezpečnost vs. přesnost
problém odvoditelnosti
přímý ptok

nepřímý útok
tracker attack

ochrana odvoditelnosti

- potlačení malých výsledků
- kombinování výsledků
- modifikace výsledků
- náhodný šum
- nýhodný výběr (random sample)
- náhodné zmatení

víceúrovňové databáze

- parcelizace
- šifrování
- integrity lock
- spolehlivý frontend (guard)
- komutativní filtr
- pohled (view)

bezpečnost v aplikačních serverech

Site

- sdílení
- složitost
- neznámý perimetr
- množství zranitelných míst
- neznámá cesta

ochrana komunikace

- proud dat
- jednotlivé zprávy

šifrování na úrovni linky
end to end šifrování
kontrola přístupu

- ochrana komunikačních portů (port protection)
- automatické zpětné volání
- odstupňovaná přístupová práva
- tichý modem (silent modem)

řízení přístupu z vnějšího prostředí
parcelizace vnitřní sítě

autentizace uzlů

autentizace v síti

- cookies
- tickets
- certifikáty, PKI
- čipové karty
- tokeny

aktivní útočník

- playback starých zpráv
- narušení služeb
- vkládání poškozených zpráv

řízení zátěže

- vycpávací zátěž (analýza zátěže)
- kontrola routování
- další metody…

Integrita dat

lokální sítě

víceúrovňová bezpečnost
spolehlivé síťové rozhraní (trusted network interface)
bezpečná komunikace

- kabely
- mikrovlny
- satelitní přenos
- celulární radio
- analogové sítě
    - X.25
    - ISDN
    - MPLS
    - pevné linky
    - X.400 message handling
      bezpečné síťové spojení