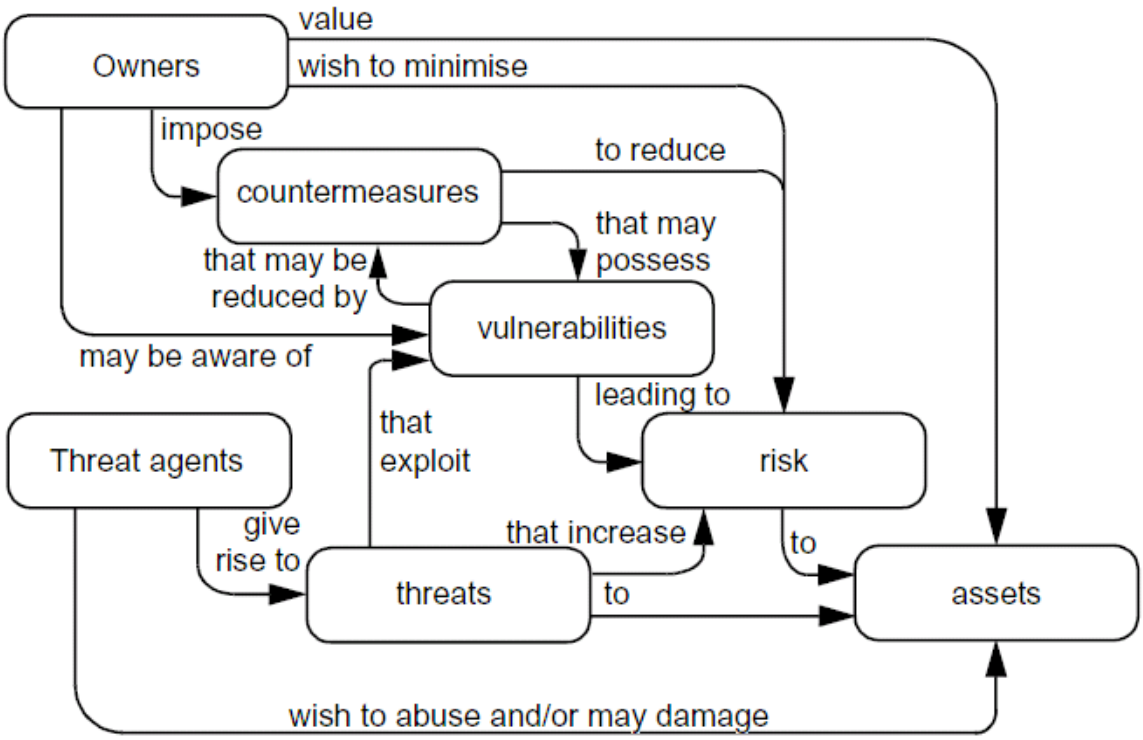
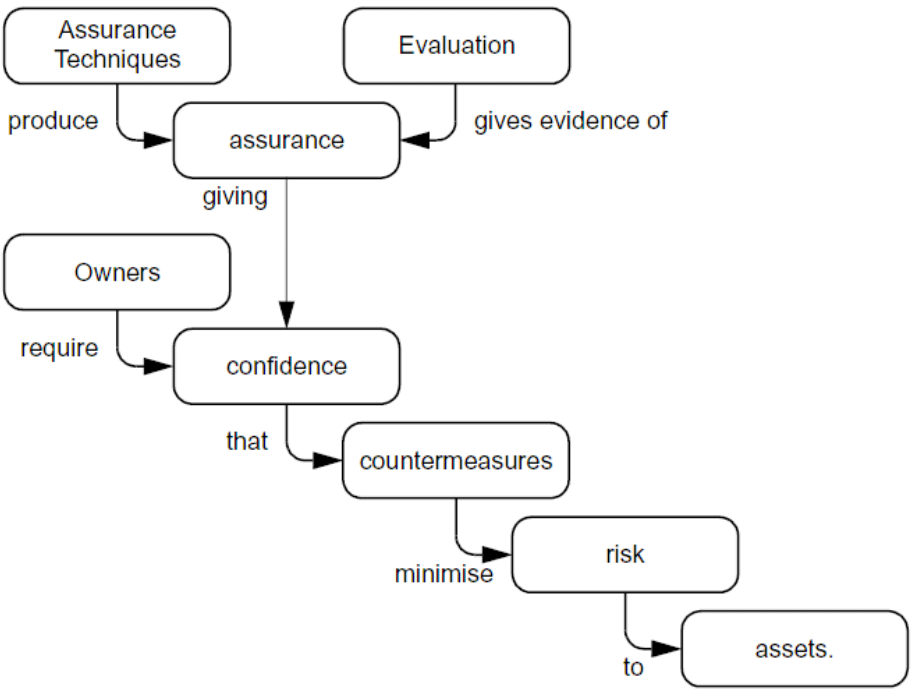
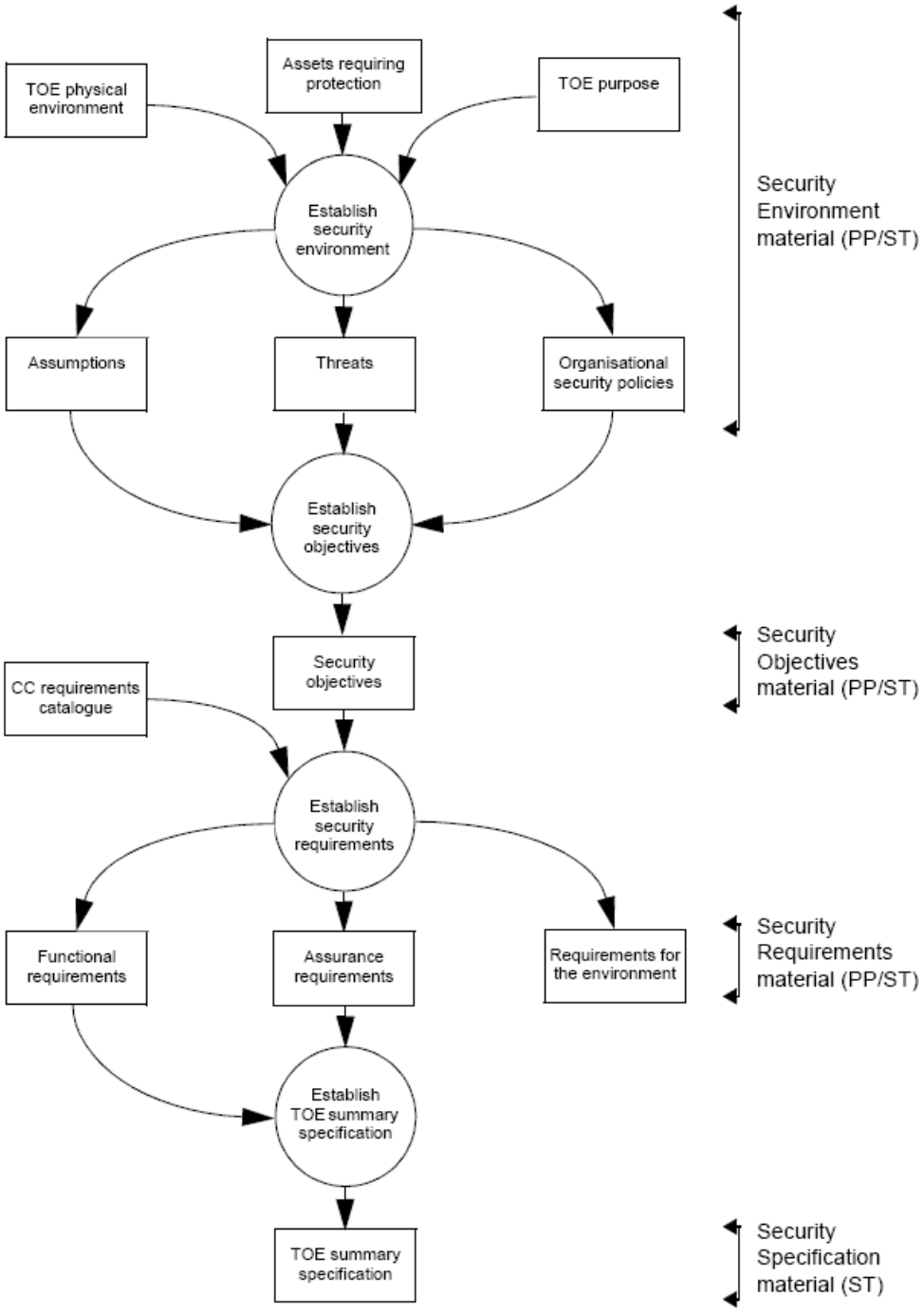
Standardizace systémů spravujících senzitivní informace







Standardy

Proč normy a standardy?

- napoví, co máte chtít a jak to má vypadat
- certifikáty o shodě s normou zajistí, že nemusíte být experty, abyste si mohli vybrat správně
- zavádějí jednotnou kulturu a stanovují srovnatelná kriteria
- normu lze použít jako vodítko, abyste na nic nezapomněli

- usnadňují audit, kontroly, jednání s partnery

Podle míry utajení a spolehlivosti, které by měl systém poskytovat je podrobován různě rigorózním testům, v kterých musí obstát. Tento proces se nazývá *validace*.
lze použít několik způsobů validace:

- formální verifikace - celý systém je popsán soustavou logických formulí, tato soustava je redukována na tvrzení o bezpečnosti systému, v rámci verifikace je třeba ověřit správnost převodu
- validace - je obecnější metoda, zahrnuje verifikaci a další metody
  - ♦ testování požadavků - testuje se, zda je splněn každý z požadavků na funkčnost systému
  - ♦ kontroly návrhu a kódu - kontroly prováděné v průběhu tvorby systému
  - ♦ testování modulů a celého systému - ověřování funkčnosti na zkušebních datech
- Tiger Team Penetration Testing - dnes opět používaná metoda, nezávislý tým odborníků pověřen úkolem provést průlom bezpečnostními mechanismy

Pokud systém obstojí při validaci, může mu být vystaven v rámci následné *certifikace* certifikát, který je formálním vyjádřením shody s požadavky příslušné normy.

Zdroje požadavků na bezpečnost:

- zákony (např. 227/2000 Sb., 148/1998 Sb., 101/2001 Sb, 440/2005 Sb.)
- oborové normy
- technické standardy
- vnitrofiremní směrnice
- požadavky obchodních partnerů
- ...

Orange Book

Trusted **C**omputer **S**ystem **E**valuation **C**riteria
tvůrcem Ministerstvo obrany Spojených států, první ucelená technická norma
systémy rozděleny do čtyř základních tříd, dále dělení na podtřídy

D, C1, C2, B1, B2, B3, A1

třída D - žádná ochrana

třída C1 - volná ochrana

Oddělení uživatelů od dat, musí existovat metody umožňující uživatelům chránit vlastní data před ostatními, uživatel zvolí, zda tyto mechanismy bude používat
IBM MVS+RACF

třída C2 - Kontrolovaný přístup

Systém stále provádí volnou ochranu zdrojů, granularita však musí být až na úroveň jednotlivých uživatelů, musí být veden access log. Navíc ochrana proti *residuím* - obsahy paměti, registrů, … poté, co proces přestane tyto používat. Residua nesmí být zpřístupněna někomu jinému.
VMS, IBM MVS+ACF2

celá třída C je označována jako *optional protection* – musí být k dispozici příslušný mechanismus, který uživatel může použít

třída B1 - značkovaná ochrana

Každý kontrolovaný subjekt a objekt musí mít přiřazen stupeň utajení a musí být tímto stupněm označen, každý přístup musí být ověřován dle Bell-LaPadula modelu, musí existovat popis implementovaného formálního modelu, systém je podrobován testování

třída B2 - Strukturovaná ochrana

musí být k dispozici verifikovatelný globální návrh systému, systém musí být rozdělen do dobře definovaných nezávislých modulů, návrh musí zohledňovat princip nejmenších možných oprávnění, bezpečnostní mechanismy musí být uplatňovány vůči všem subjektům a objektům včetně všech zařízení, musí existovat analýza možných skrytých kanálů
vlastní systém musí běžet v rámci své bezpečnostní domény a provádět kontroly své integrity
Multics

třída B3 - Bezpečnostní domény

Systém musí být podrobitelný extenzivnímu testování, musí existovat úplný popis celkové struktury návrhu systému, musí být konceptuálně jednoduchý

musí existovat ochranné mechanismy na úrovni jednotlivých objektů, každý přístup musí být testován, kontrola na úrovni provádění jednotlivých typů přístupu daného subjektu
Systém musí být vysoce odolný vůči průnikům. Zařízení provádějící audit log musí umět odhadnout hrozící nebezpečí.

celá třída B je zonačována jako *mandatory protection* – musí být k dispozici odpovídající mechanismus, který uživatel nemůže obejít ani deaktivovat

tříba A1 - Verifikovaný návrh

Návrh systému musí být formálně verifikován, existuje formální model bezpečnostního mechanismu s důkazem konzistentnosti, formální specifikace systému s ověřením, že odpovídá formálnímu modelu, ověření, že implementace není odchylná od formální specifikace, formální analýza skrytých kanálů
SCOMP, patrně KVM/370, PSOS, KSOS

ITSEC

The **I**nformation **T**echnology **S**ecurity **E**valuation **C**riteria
mezinárodní sada kriterií, nadmnožina TCSEC
kriteria rozdělena na třídy funkčnosti (F) a korektnosti (E)
třídy funkčnosti F-D, F-C1, F-C2, F-B1, F-B2 a F-B3 zhruba co do funkčnosti odpovídají třídám C1 až B3 hodnocení TCSEC
kriteria hodnocení funkčnosti rozdělena na hodnocení integrity systému (F-IN), dostupnosti systémových zdrojů (F-AV), integrity dat při komunikaci (F-DI), utajení komunikace (F-DC) a bezpečnosti v rámci celé sítě (F-DX)
každé z těchto kriterií může být vyhodnocováno nezávisle, vyhodnocování prováděno pro požadovanou třídu funkčnosti

kriteria pro hodnocení korektnosti přidána pro zvýšení důvěryhodnosti systému
požadavky vyšší třídy korektnosti vždy nadmnožinou předchozích
E1 - testování
E2 - kontrola konfigurace a distribuce
E3 - ověření detailního návrhu a zdrojového kódu
E4 - zevrubná analýza slabin systému
E5 - důkaz, že implementace odpovídá detailnímu návrhu
E6 - formální modely, formální popisy a jejich vzájemná korespondence
tyto třídy odpovídají požadavkům na důvěryhodnost kladeným třídami C2 až A1 hodnocení TCSEC

kromě zmíněných kriterií hodnocení zabezpečených systémů existuje celá řada norem a doporučení upravující prakticky všechny podstatné rysy chování a architektury těchto systémů

Common criteria

metanorma stanovující principy a postupy, jak odvozovat konkrétní technické normy pro vývoj, testování, výsledné vlastnosti a provoz technických bezpečnostních protiopatření v různých prostředích
úzce souvisí s materiálem Common Evaluatin Methodology – pravidla pro vyhodnocování konkrétních systémů (target of evaluation) vůči daným požadavkům
formalizuje proces vyhodnocování:
evaluační kriteria → evaluační metodologie → evaluační schéma → evaluace → výsledky evaluace → certifikace → registr certifikátů
vyžaduje síť zkušebních laboratoří
odděluje funkcionalitu (sec. functional requirements) od „jistoty“ (sec. assurance req.)
sada konkrétních funkčních a „jistotních“ požadavků tvoří *profil zabezpečení (protectin profile)*
Funkční (functional) třídy:

- FAU – bezpečnostní audit
- FCO – komunikace
- FCS – kryptografická podpora
- FDP – ochrana uživ. dat
- FIA – identifikace a autentizace
- FMT – bezpečnostní management
- FPR – soukromí
- FTP – ochrana bezp. mechanismu
- FRU – využívání prostředků
- FTA – přístup
- FTP – důveryhodná cesta/kanál

Jistotní (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 v rámci evaluačních kriterií potom podléhá následující klasifikaci:

- APE – vyhodnocení profilu bezpečnosti
- ASE – vyhodnocení cíle hodnocení

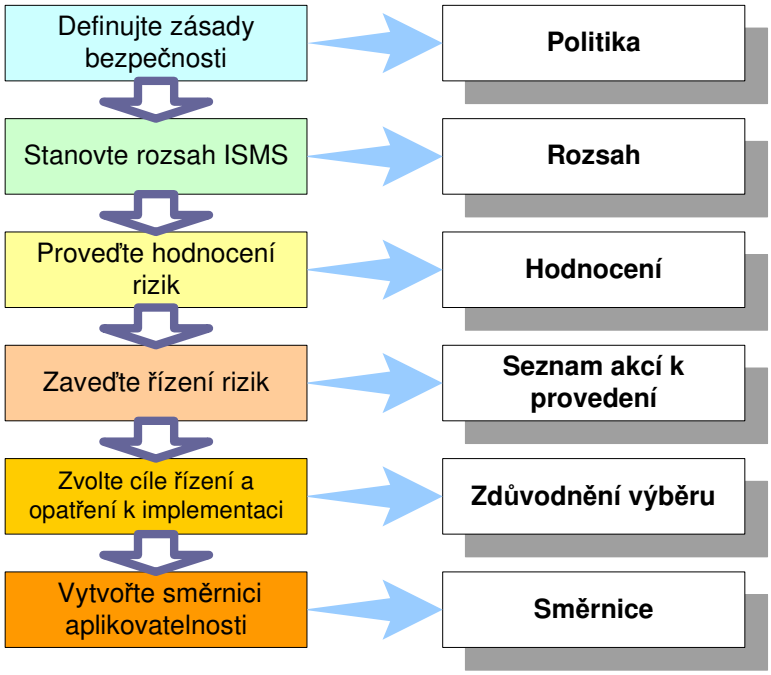
Úrovně vyhodnocení (eval. assurance level) dle kriterií:

- 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

BS7799

(ISO IEC TR 17799, ISO 27000) organizační norma, která popisuje obecně, jaké činnosti musí organizace vykonávat pro zajištění bezpečnosti IS, nestanoví kvalitativní kriteria
založena na myšlence budování bezpečnosti shora dolů tj. od bezpečnostní politiky po implementaci protiopatření
předpokládaný proces tvorby bezpečnosti a z něho odvozené bezpečnostní dokumentace ukazuje obrázek



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)

Pro podporu budování bezpečnosti a návrhu implementace bezpečnostních mechanismů podle BS7799 existuje standardní metodika a automatizovaný nástroj CRAMM.

Federal Information Processing Standard

FIPS 140-1: Security Requirements for Cryptographic Modules, January 4, 1994.
FIPS 140-2: Security Requirements for Cryptographic Modules, May 25, 2001. Change Notices 2, 3 and 4: 12/03/2002

Standardy PKCS

vytvářeny v laboratořích firmy RSA Security (dříve RSA)
představují ucelený soubor technických norem popisujících implementaci různých nástrojů asymetrikcé kryptografie
původně proprietární normy, dnes široce používaný de-facto standard
PKCS #1:RSA Cryptography Standard
PKCS #3:Diffie-Hellman Key Agreement Standard
PKCS #5:Password-Based Cryptography Standard
PKCS #6:Extended-Certificate Syntax Standard
PKCS #7:Cryptographic Message Syntax Standard
PKCS #8:Private-Key Information Syntax Standard
PKCS #9:Selected Attribute Types
PKCS #10:Certification Request Syntax Standard
PKCS #11:Cryptographic Token Interface Standard
PKCS #12:Personal Information Exchange Syntax Standard
PKCS #13: Elliptic Curve Cryptography Standard
PKCS #15: Cryptographic Token Information Format Standard

Zdroje standardů

Mezinárodní standardizační instituty

ISO - International Organization for Standardization http://www.iso.ch/
IEC - International Electrotechnical Commission http://www.iec.ch/
ITU - International Telecommunication Union http://www.itu.ch/
WSSN - World Standards Services Network http://www.wssn.net/

Regionální standardizační instituty

CEN - European Committee for Standardization http://www.cenorm.be/

CENELEC - European Committee for Electrotechnical Standardization
http://www.cenelec.org/
COPANT - Pan American Standards Commission http://www.copant.org/
ETSI - European Telecommunications Standards Institute http://www.etsi.org/

Formální modely bezpečnosti

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 modely

jsou vhodné případy, kdy stačí jednoduché ano/ne rozhodování, zda danému subjektu poskytnout přístup k požadovanému objektu a není nutné pracovat s klasifikací dat !všechna data stejná!

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

```
if profit <= 0
   then delete file F
   else
      write file F, "_zpráva_"
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

Víceúrovňové modely

v předchozích modelech jsme měli jednoduché vztahy objekt je/není senzitivní, subjekt má/nemá přístup k danému objektu
obecně však může být několik stupňů senzitivity a "oprávněnosti"
tyto stupně senzitivity se dají použít k algoritmickému rozhodování o přístupu daného subjektu k cílovému objektu, ale také k řízení zacházení s objekty
víceúrovňový systém „rozumí" senzitivitě dat a chápe, že s nimi musí zacházet v souladu s požadavky kladenými na daný stupeň senzitivity
(např. tajná data ukládáat pouze na konkrétní diskové pole, přísně tajná data posílat mimo systém výhradně zašifrovaná HW šifrátorem, ...)
rozhodnutí o přístupu pak nezahrnuje pouze prověření žadatele, ale též klasifikaci prostředí, ze kterého je přístup požadován (tj. uživatel je prověřen na vyhrazená data, ale sedí u stanice, která nemá klasifikaci „na vyhrazená data" a tudíž přístup není povolen).

Military security model

u zelených mozků je každá informace zařazena do některé z kategorií utajení (např. *unclassified, confidental, secret, top secret*), které jsou disjunktní
silné uplatnění zde má *princip nejmenších privilegií* - každý subjekt má mít pouze taková oprávnění, aby mohl konat svoji práci
všechny chráněné informace jsou rozděleny podle obsahu do *oblastí* (compartments), informace může být i několika oblastech zároveň
klasifikací informace potom rozumíme dvojici <*stupeň_utajení*, *oblasti*>
aby subjekt mohl používat požadovanou informaci, musí mít dostatečné *oprávnění*.
oprávnění má stejný tvar jako klasifikace - <*stupeň_utajení*, *oblasti*>, tedy daný subjekt smí používat informace až do *stupeň_utajení* v těchto *oblastech.*

$$O \leq S \Leftrightarrow st\_utaj_O \leq st\_utaj_S \wedge oblast_O \subseteq oblast_S$$

Relace $\leq$ odpovídá *oprávnění* subjektu *S* k danému objektu *O*.
Požadavky na stupeň utajení bývají označovány jako hierarchické, rozdělení na oblasti jako nehierarchické omezení.

Svazový model (Lattice model)

předchozí military model je specielním případem tohoto modelu
relace $\leq$ je částečným uspořádáním, množina klasifikací všech informací v systému tvoří svaz, stejně tak množina oprávnění všech subjektů
v různých oblastech se používá různých svazů, např. v komerční oblasti jsou obvyklé stupně utajení *public, company confidental, high security*, rovněž rozdělení do oblastí se liší případ od případu …
svazový model je často používaným modelem v mnoha prostředích

dále popíšeme dva modely, zabývající se tokem informací uvnitř systému

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

$$C(O) \leq C(S)$$

**-vlastnost* (*-Property):

Subjekt *S* mající právo čtení k objektu *O* může zapisovat do objektu *P* právě když

$$C(O) \leq C(P)$$

Obyčejně nepotřebujeme tak silná omezení, která klade **-vlastnost*. Často je tato vlastnost poněkud oslabena v tom smyslu, že systém povolí zápis do objektu nižší bezpečnostní třídy, pokud zapisovaná data nezávisí na čtených údajích.
Model byl je používán v systémech, které paralelně zpracovávají informace různého stupně utajení.

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

$$I(O) \leq I(S)$$

*Integritní *-vlastnost* (Integrity *-Property):

Subjekt *S* mající právo čtení k objektu *O* může zapisovat do objektu *P* právě když

$$I(O) \geq I(P)$$

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.

Modely pro různé účely

Clark-Wilson model

dobře odpovídá potřebám komerčních organizací, přejímá postupy běžné v účetnictví
základní principy:

1. dobře formované transakce (konzistentní data → konzistentní data)
2. separace operací – žádnou operaci nesmí být schopen korektně provést jediný subjekt

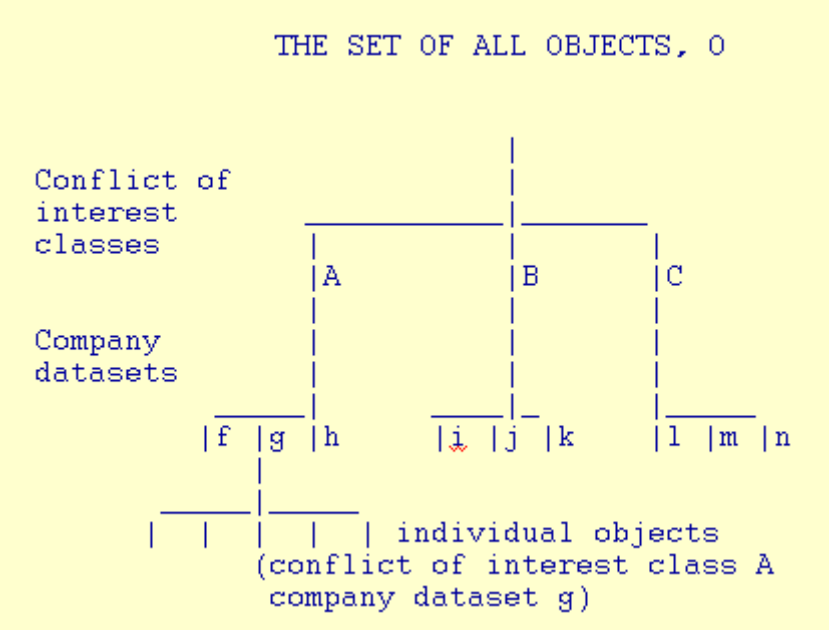
pravidla modelu rozdělujeme obvykle na požadavky na korektnost „C“ a na vynucení „E“
C1 – Všechny procedury testující validitu dat musí zajistit, že pokud doběhnou, všechna chráněná data jsou korektní.

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 operací.
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)

Představuje příklad dynamického modelu – 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 skupin (conflict of interest classes)
sanitizovaná informace – odstraněny ty části, které umožňují identifikovat konkrétního vlastníka



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 skupiny

**-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

Závěrem dva teoretické modely pro modelování správy oprávnění

Graham-Denning model

model pracuje s množinou subjektů *S,* množinou objektů *O*, množinou práv *R* a přístupovou maticí *A*.
Každý objekt má přiřazen jeden subjekt nazývaný *vlastník,* každý subjekt má přiřazen jiný subjekt nazývaný *kontroler*.
Model definuje následující práva:

- *vytvořit objekt* - povoluje subjektu vytvořit v systému nový objekt
- *vytvořit subjekt*, *zrušit objekt*, *rušit subjekt* - obdobně jako předchozí

- *číst přístupová práva* - povoluje subjektu zjistit aktuální přístupová práva jistého subjektu k určitému subjektu
- *přidělit přístupová práva* - dovoluje vlatníku objektu přidělit jistá práva k objektu určitému subjektu
- *zrušit přístupová práva* - dovoluje vlastníku objektu resp. kontroleru subjektu odebrat danému subjektu jistá práva k objektu resp. subjektu
- *předat přístupová práva* - dovoluje subjektu předat některé ze svých práv jinému subjektu (každé oprávnění může být předatelné či nikoliv, obdrží-li subjekt předatelné právo, může jej dále předat jako předatelné či nepředatelné).

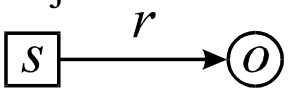
Následující tabulka uvádí podmínky nutné pro vykonání operací s přístupovými právy.

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 $A[x,o]$

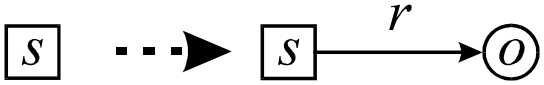
*r** označuje předatelné právo

Take-Grant system

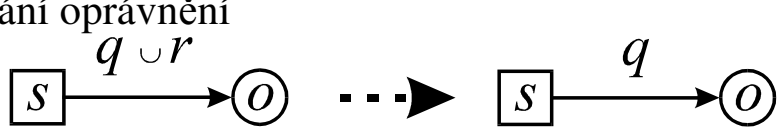
model pracuje s čtyřmi základními primitivami: *create, revoke, take, grant.*
předpokládáme, že systému obsahuje množinu subjektů *S,* množinu objektů *O*, objekty dělíme na aktivní (zároveň i subjekty) a pasivní (nejsou subjekty) a množinu práv *R*
Pro popis operací použijeme následující notaci:



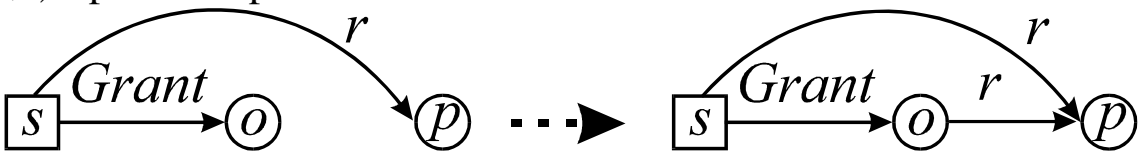
Subjekt *s* má k objektu *o* oprávnění *r*.
create(o,r) - vytvoření objektu



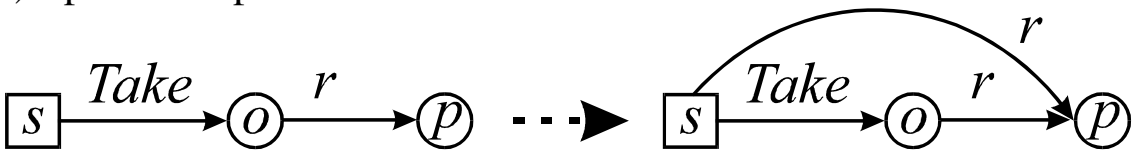
revoke(o,r) - odebrání oprávnění



grant(o,p,r) - předání oprávnění



take(o,p,r) - převzetí oprávnění



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

Bezpečnostní 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.

Všechno je otázka míry

Bezpečnostní politika vám říká, jak zvládnout problém zajištění IS proti incidetnům.

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

umožní rozmyslet si, kde vás bota tlačí
materiál by neměl popisovat neexistující systém (zkoumaný IS se v průběhu zkoumání vyvíjí)

Organizace pohybující se ve stejné branži budou mít podobné nároky na bezpečnost

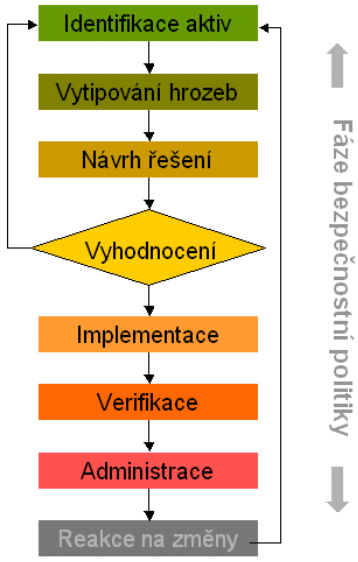
Výhody existence BP

stejně jako každá činnost, i provozování systému pro správu informací je spojeno s jistým rizikem (chyba zařízení, obsluhy, programu, vandalismus, krádež, …)
provedení kvalifikovaného odhadu rizik přináší:

- zlepšení obecného povědomí - pracovníci si problém uvědomí a mají šanci jej pochopit
- identifikace hodnot, slabin a možných kontrol celého systému - ne vždy je jasné, které části systému mají největší hodnotu, odkud pramení největší nebezpečí
- zlepšení východiska pro strategická rozhodnutí - některé ochranné a kontrolní mechanismy velmi snižují produktivitu systému přičemž jejich přínos není zřejmý, různé druhy nebezpečí jsou různě reálné a představují mnohdy daleko větší hrozbu, než by se dalo očekávat
- lepší rozložení výdajů na bezpečnost - některé velmi drahé ochranné mechanismy poskytují pouze malé zvýšení bezpečnosti a popřípadě i naopak

Jak na to

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



Identifikace a odhad aktiv

Základem je zjistit, co vlastně ve svém informačním systému mám a k čemu je to dobré

... nikdo neví, kde fyzicky server leží, co dělá ta modrá krabice v rohu ... co se stane, když tenhle kus přestane fungovat ...

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
- data - vlastní uložená data, logy, archivní kopie, listingy, …
- lidé - pracovníci potřební k správnému chodu systému, správci, programátoři

- dokumentace - programů, technického vybavení, systému, administrativní postupy
- spotřební materiál - papír, diskety, tonery, pásky do tiskáren, …
- zákazníci
- image společnosti
- ... atd. Zjevně každý si musí vymyslet vlastní seznam.

V podstatě v tomto kroku provedeme zevrubnou inventarizaci celéh systému. Cena některých částí může být pouze velmi přibližně odhadnuta a i takový odhad může být velmi obtížný.

Vytipování hrozeb

je potřeba určit, co nás bude stát realizovaný bezpečnostní incident

zkoumáte:

- 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
- 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

Dotazníček			
Hodnota	*Utajení*	*Integrita*	*Dostupnost*
Hardware		přetížení, zničení, poškození	
Software	odcizen, kopírován	modifikován	smazán, přesunut
Data	zpřístupněna vně firmy	zničena chybou SW ; HW ; lidí	smazána
Lidé			únava, nemoc
Dokumentace			ztracena, odcizena

Zjišťování těchto faktů lze provádět formou dotazníku, který vyplní zainteresovaní pracovníci (viz. obrázek).

Odhad pravděpodobnosti zneužití

zjistíme, jak často dojde ke zneužití některé z expozic systému

pomáhá přemýšlet o věci nikoliv jako o pravděpodobnosti, ale jako o četnosti

když ani toto nepomáhá (jak často přijde do Prahy tisíciletá voda), lze použít některou z následujících metod:

- Odhad na základě obecných dat - např. pojišťovny mají rozsáhlé záznamy o počtu katastrof a o průměrných způsobených škodách, výrobci mají 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

Frekvence	*Hodnocení*	*Frekvence*	*Hodnocení*
více než 1 x za den	10	1 x za měsíc	5
1 x za den	9	1 x za 4 měsíce	4
1 x za 3 dny	8	1 x za rok	3
1 x za týden	7	1 x za 3 roky	2

- *Delfská metoda* - okruh hodnotitelů provede hodnocení dané veličiny. Poté je každý seznámen s výsledky ostatních a upraví své hodnocení. Pokud jsou upravená hodnocení podobná, máme výsledek, v opačném případě výsledek vznikne dohodou hodnotitelů.

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

Poté, co jsme zjistili, jaké jsou naše problémy, je 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.

když jde o peníze, musí zhusta city stranou.

Návrh řešení / Přehled použitelných ochranných mechanismů

Když je třeba zavést nové ochranné mechanismy:

Můžete

- probrat jednotlivé expozice systému a zkoumat možnosti jejich pokrytí
- mezi všemi ochrannými mechanismy hledat nějaký, který by řešil náš problém.

uvažte, že stejně nevyrazíte ze svého IS nic, co by sám od sebe neuměl

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

1. Statement (záměr bezpečnosti) – cca 1 strana základního záměru, podepsaná top managementem
2. Politika a principy bezpečnosti – podle potřeby i desítky stran
3. Navazující dokumenty a směrnice (viz níže) – dokumenty různé povahy, srozumitelné pro uživatele, nebo vysoce technické pro administrátory, dodavatele apod., v případě rozsáhlé organizace i tisíce stran

- popis celkových cílů bezpečnostních aktivit - např ochrana dat před katastrofami, před úniky mimo organizaci, apod.
- 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, těmto lidem důkladně vysvětlit jejich úkol a důvody

též je nutné navrhnout způsob hodnocení splnění těchto úkolů
možné rozdělení zodpovědnosti:

- uživatelé osobních počítačů - každý ručí za svůj počítač
- administrátor databázového systému - zodpovídá za přístup k datům a jejich integritu
- firma může pověřit zvláštního pracovníka zodpovědného za vytvoření obecných pravidel práce s daty a jejich uvolňování či rušení
- pracovníci osobních oddělení zodpovídají za přijetí důvěryhodných a spolehlivých pracovníků

Časový rozvrh

některá opatření mohou být příliš nákladná, nebo složitá, než aby mohla být zavedena naráz
musí existovat plán, do kdy budou která opatření zavedena, případně nejzajší termíny splnění jednotlivých fází bezpečnostního plánu
též pořadí zavádění opatření může být důležité

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