Použití formálních modelů a standardních řešení

Jakou bezpečnost budovat
Použití formálních modelů bezpečnosti
Klasifikace informací a práce s nimi

Klasifikované informace musí být řízeny aby:

- zabráněno neautorizovanému a nesprávnému přístupu
- podpořena analýza průniků a úniků
- vynucován "need to know" princip

Je nezbytný standard kontroly a řízení.

Princip "Need to Know"

Pracovník získá přístup

- pouze protože „potřebuje znát“ pro svoji práci
- ne protože by bylo pohodlné, aby věděl
- ne na základě svého postavení, pozice, úrovně prověření, ...

Princip platí obecně na vnitřní i vnější osoby

Princip "Need to Retain"

Klasifikované dokumenty by měly být uchovávány pouze po dobu použití, pak musí být smazány, nebo vráceny vlastníkovi.

- omezit držení materiálů na minimum
- roční kontrolu držení níže klasifikovaných materiálů
- pravidelné kontroly všech výskytů výše klasifikovaných materiálů
- uložení výše klasifikovaných materiálů v identifikovatelných složkách

Pracovní procedury

- bezpečnostní zóny – vytvoření zón a kontrola pohybu pracovníků
- bezpečnost místností – ochrana uložených a používaných materiálů, uzavření prostor, opuštění místa a místnosti, open-plan místnosti
- Clear Desk and Clear Screen Policy
- End of Day Procedures

Příprava a zpracování informací

- jaké klasifikované informace jsou udržovány
- jaká je požadovaná úroveň ochrany
- kde jsou
- kdo je autorizován, u vyšších stupňů i kdo byl autorizován

Příprava

- založit oddělené produkční a kopírovací zdroje
- evidovat počty kopií
- likvidace nepovedených exemplářů
- proškolení personálu.

Registrace

klasifikované dokumenty by měly obsahovat identifikaci autora a čas vzniku
číslování kopií, stránek, počty stránek, ...

"Accountable" dokumenty

držitel dokumentu musí pravidelně ověřovat a potvrzovat správně zacházení
autor určí zda dokument podléhá tomuto režimu a interval kontrol

Minimum Standards for Controlling TOP SECRET and SECRET Material

71. The minimum standards for controlling TOP SECRET and SECRET material are:

- record its location on preparation, arrival into the organisation, in use and in storage
- record its disposal or destruction
- keep these records for at least five years.

72. For further guidance on controlling TOP SECRET and SECRET material, see the NZSIS *Protective Security Manual*.

Copying, Printing and Facsimile Machines

75. To prevent unauthorised use, strictly control access to copying machines and printers, including microfilming equipment, and facsimile machines that are not protected by COMSEC systems.

76. Control depends on the circumstances and types of machines. When a machine is used to copy or print substantial quantities of classified material, control its use during working hours and immobilise it at all other times.

Review

82. In addition to routine document destruction, organisations should periodically hold special destruction exercises. These exercises should:

- ruthlessly cull unwanted copies of classified documents, especially when master sets or originals exist, for example at head office
- take care, however, not to destroy original documents of historical value (see paragraph 0).

Spot Checks

83. Spot checks deter taking TOP SECRET and SECRET documents out of the office for unauthorised purposes.

84. Line managers should carry out spot checks:

- without warning
- at frequent but irregular intervals
- during normal working hours.

85. To prevent spot checks from degenerating to a tiresome chore:

- check only TOP SECRET and SECRET documents
- check only a few documents at a time.

86. For further advice on spot checks, see the NZSIS *Protective Security Manual*.

Custody of Classified Material

General

88. Chief Executives or heads of government departments and agencies, State Owned Enterprises and Crown Entities determine the security arrangements for storing IN CONFIDENCE, SENSITIVE and RESTRICTED material.

89. CONFIDENTIAL, SECRET and TOP SECRET material must be locked in security containers when not in use.

90. CONFIDENTIAL, SECRET and TOP SECRET material should not be stored together with UNCLASSIFIED material.

91. IN CONFIDENCE, SENSITIVE and RESTRICTED material may be stored together with UNCLASSIFIED material.

92. When storing material of different classifications together, use the security standard of the highest-classified item.

Minimum Standards for Holding Material Classified CONFIDENTIAL or Above

93. Minimum standards for holding material classified CONFIDENTIAL have been established. They are based on:

- the security container and its lock
- the position or site of the container
- the use of approved security equipment.

Transporting Classified Material

95. During transit, classified material is at risk from accidental or deliberate compromise.

96. To protect classified material when in transit:

- use reliable means of transport
- use robust packaging
- conceal the attractiveness, identity and source of the material, under plain cover.

97. With higher levels of classification, use an audit system to track the material and reveal any actual or attempted tampering.

98. Protect classified material in transit:

- within and between sites and establishments in New Zealand
- between New Zealand and countries overseas
- within and between countries overseas.

Minimum Requirements for Transmission and Transport

Level	*Classified Information*	*Classified Equipment*
IN CONFIDENCE	Handle, use and transmit with care. See Chapter 3 Annex A.	Control, use and transport with care.
SENSITIVE or RESTRICTED	Handle, use and transmit with care. Take basic precautions against accidental compromise or opportunist attack.	Control, use and transport with care. Take basic precautions against accidental compromise or opportunist attack.

	See Chapter 3 Annex B and C.	
CONFIDENTIAL	Handle, use and transmit to make accidental and deliberate compromise unlikely. Where possible, make actual or attempted compromise unlikely. Where possible, make actual or attempted compromise likely to be detected. See Chapter 3 Annex D.	Control, use and transport to make accidental compromise unlikely. Offer a degree of resistance to deliberate compromise. Control knowledge of planned movements. Make actual or attempted compromise likely to be detected.
SECRET	Handle, use and transmit to minimise the chance of accidental compromise. Offer a degree of resistance to deliberate compromise by a professional attack. Where possible, detect actual or attempted compromise and help identify those responsible. See Chapter 3 Annex E.	Control, use and transport to minimise the possibility of accidental compromise. Offer a degree of resistance to deliberate compromise by a professional attack. Limit knowledge of planned movements. Detect actual or attempted compromise and help identify those responsible.
TOP SECRET	Handle, use and transmit to prevent accidental compromise. Offer a degree of resistance to compromise by a sustained and sophisticated attack. Where possible, detect actual or attempted compromise and make it likely that those responsible will be identified. See Chapter 3 Annex F.	Control, use and transport with every possible precaution against accidental damage. Offer a degree of resistance to deliberate compromise by a sustained and sophisticated attack. Strictly limit knowledge of planned movements to those with a "need to know". Detect actual or attempted compromise and make it likely that those responsible will be identified.

Destruction of Classified Material

107. Until classified material has been reduced to a state where it cannot be read or reconstituted, it retains its classification. Procedures for handling, recording, transmitting, and destroying classified waste are the same as for any material with that classification.

Record of Destruction

Keep a record of the destruction of TOP SECRET and accountable documents.

- the date
- the signature of the person carrying out the destruction
- the authority for the destruction
- for TOP SECRET material, the signature of a second witness to the destruction.

Before destroying any file, folder or document, first verify that all TOP SECRET and accountable pages and enclosures are present and complete.

Modely bezpečnosti

popisují způsob, jak je v systému nakládáno a informacemi
zabývají se pouze automatickými transfery

Jednoúrovňové modely

jsou vhodné pouze pro případy, kdy stačí jednoduché rozhodování, zda danému subjektu poskytnout přístup k požadovanému objektu

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 růných 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. Bezpečnostní třída entity v podstatě 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. Následující modely se zabývají teoretickými limity abstraktních bezpečnostních systémů.

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.

Modely pro budování bezpečnosti

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.

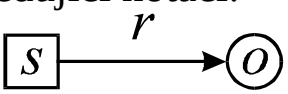
vytvořit objekt *o*	-
vytvořit subjekt *s*	-
zrušit objekt *o*	vlastník je v $A[x,o]$
zrušit subjekt *s*	vlastník je v $A[x,s]$
číst přístupová práva *s* k *o*	kontroler je v $A[x,s]$, nebo vlastník v $A[x,o]$

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*]

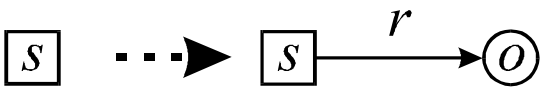
*r** označuje předatelné právo

Take-Grant system

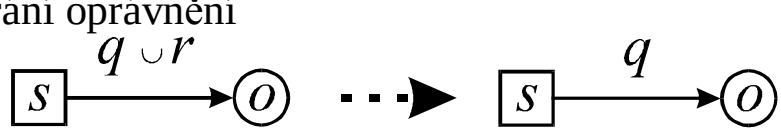
model pracuje s čtyřmi základními primitivami: *create, revoke, take, grant.*
předpokládáme, že systému obsahuje množinu subjektů *S*, množinu objektů *O*, objekty dělíme na aktivní (zároveň i subjekty) a pasivní (nejsou subjekty) a množinu práv *R*
Pro popis operací použijeme následující notaci:



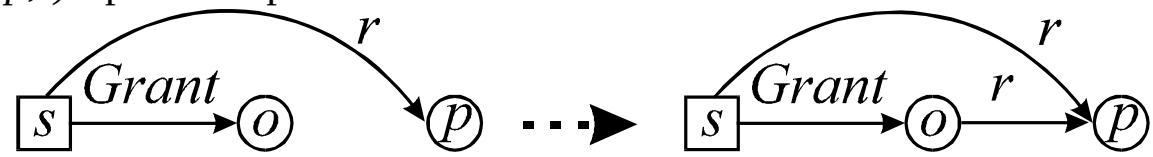
Subjekt *s* má k objektu *o* oprávnění *r*.
create(o,r) - vytvoření objektu



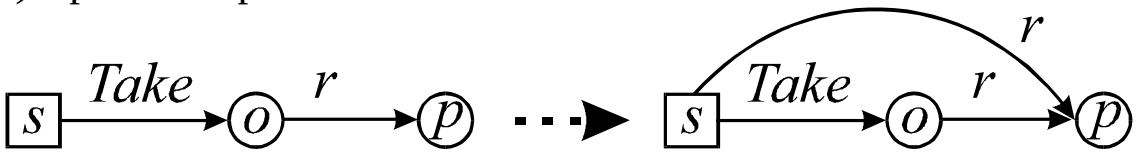
revoke(o,r) - odebrání oprávnění



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.