Politique de sécurité

Master SEMS, 2012-2013

Pierre Paradinas

November 4, 2012

Exemple de politique de sécurité

Messagerie (liste de diffusion) de l'Université d'Illinois

- L'usage de liste de diffusion est autorisé sous les conditions suivantes :
  - 1. Toutes listes de diffusion comprenant plus de 100 destinataires doit avoir :
    - ⋆ l'aval du doyen (ou d'un représentant) si l'ensemble des destinataires comprend des étudiants qui n'appartiennent pas au groupe des administrateurs de la liste de diffusion,
    - ⋆ l'aval du vice-président de l'université ou du service des ressources humaines si l'ensemble des destinataires comprend des employés qui n'appartiennent pas au groupe des administrateurs de la liste de diffusion,
  - 2. le contenu du message doit être inclus dans le message lui-même et pas en pièce jointe dans la mesure du possible,
  - 3. le message doit préférentiellement contenir des liens plutôt que des pièces jointes afin d'éviter d'augmenter la taille du message.

Exemple de politique de sécurité (suite)

Messagerie (liste de diffusion) de l'Université d'Illinois

- L'usage des emails est interdit dans les contextes suivants (liste non exhaustive) :
  - 4. l'objectif du message envoyé viole une loi fédérale,
  - 5. le message est à caractère commercial,
  - 6. l'identité de l'émetteur n'apparaît pas,
  - 7. l'envoi de masse congestionnant le réseau,
  - 8. la diffusion de messages inappropriés à des listes ou des individus,
  - 9. attribution d'une priorité « élevée » à un message envoyée sur une liste de diffusion,
  - 10. ...

Remarques

Que pouvez vous dire de cette politique de sécurité ?

Exemple de politique de sécurité (suite)

- Règles sans ambiguïté (règles 1 à 6)
- Régles sujet à interpétation (régles 2 et 8)
- Règles en conflit ?
  - Par exemple, si le doyen souhaite envoyer un message urgent à l'ensemble de l'université
    - ⋆ la règle 1 l'autorise alors que la règle 9 l'interdit
    - ⋆ et la liste est pas exhaustive

Remarques

Une politique (réglement de sécurité) requiert des définitions formelles au delà du langage naturel pour permettre d'avoir un moyen de décider la conduite à tenir sans ambiguïté.

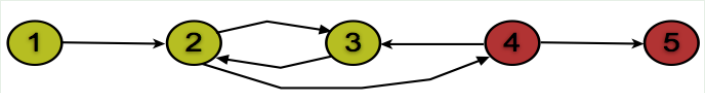
Politique de sécurité (définitions)

Définitions

Une politique de Sécurité définit pour un système un ensemble d'état sûrs (autorisés) et un ensemble d'état non sûrs (non autorisés).
Un système sécurisé est un système qui part d'un état (du système) sûrs et qui n'entre jamais dans un état non sûrs.

Exemple

Example : Les états 1, 2 & 3 sont des états sûrs. Les états 4 et 5 ne le sont pas.
Le système est il sûr ou non sûr ?
Comment rendre le système sûr ?



Politique de sécurité (définitions et solution)

Exemple

Example : Les états 1, 2 & 3 sont des états sûrs. Les états 4 et 5 ne le sont pas.
Comment rendre le système sûr ?

Politique de sécurité (définitions)

Définition

Une *rupture* de sécurité apparait quand un système entre dans un état non sûr (non autorisé).

Les différents types de ruptures se réfèrent à ce qui a été vu avant au travers des propriétés de sécurité (confidentialité, intégrité et disponibilité).

Confidentialité

Soit X un ensemble d'entités et I un ensemble d'information. I a la propriété de confidentialité vis à vis de X, si et seulement si aucun élément de X à la connaissance de l'information I.

Politique de sécurité (définitions)

Définition

Une *rupture* de sécurité apparait quand un système entre dans un état non sûr (non autorisé).

Les différents types de ruptures se réfèrent à ce qui a été vu avant au travers des propriétés de sécurité (confidentialité, intégrité et disponibilité).

Confidentialité

Soit X un ensemble d'entités et I un ensemble d'information. I a la propriété de confidentialité vis à vis de X, si et seulement si aucun élément de X à la connaissance de l'information I.

Politique de sécurité (définitions)

Définition : Intégrité

Soit X un ensemble d'entités et I un ensemble d'information et de ressources. I a la propriété d'intégrité vis à vis de X, si et seulement si tout les entités de X font confiance à I (information non modifiée (intègre) dont la source est aussi de la confiance (authenticité)).

Définition : Disponibilité

Soit X un ensemble d'entités et R un ensemble de ressources. R a la propriété de disponibilité vis à vis de X, si et seulement si tout élément de X peut accéder à tout élément de R.

Politique de sécurité (définitions)

Définition : Intégrité

Soit X un ensemble d'entités et I un ensemble d'information et de ressources. I a la propriété d'intégrité vis à vis de X, si et seulement si tout les entités de X font confiance à I (information non modifiée (intègre) dont la source est aussi de la confiance (authenticité)).

Définition : Disponibilité

Soit X un ensemble d'entités et R un ensemble de ressources. R a la propriété de disponibilité vis à vis de X, si et seulement si tout élément de X peut accéder à tout élément de R.

le cnam

Mécanismes de sécurité (définitions)

Définition : renforcer la politique de sécurité

Un mécanisme de sécurité est un ensemble de règles, mesures et/ou procédures dont l'objectif est d'appliquer la politique de sécurité.

Exemple

Les données confidentielles ne peuvent être dupliquées de manière non contrôlées (règles).
Les sauvegardes (de données) doivent être dans des lieux différents de l'usage habituel des données (procédures).

Mécanismes de sécurité (définitions)

Définition : renforcer la politique de sécurité

Un mécanisme de sécurité est un ensemble de règles, mesures et/ou procédures dont l'objectif est d'appliquer la politique de sécurité.

Exemple

Les données confidentielles ne peuvent être dupliquées de manière non contrôlées (règles).
Les sauvegardes (de données) doivent être dans des lieux différents de l'usage habituel des données (procédures).

le cnam

Typologie des politiques de sécurité

Définition

Chaque contexte et/ou organisation a ses propres besoins ainsi que ses propres “niveaux” de confidentialité, intégrité et disponibilité.

- Les politiques de sécurité militaire sont essentiellement centrées sur la confidentialité.
- Les politiques de sécurité commerciale (industrielle) sont essentiellement centrées sur l'intégrité et la disponibilité.

Remarque

Cette distinction paraît moins d'actualité !
Pour les militaires, il y a beaucoup d'applications qui réclament de l'intégrité (pour le renseignement) et de la disponibilité (des systèmes).
Le carnet de commande Apple chez TSMC ou Samsung n'est pas publique, de plus dans des entreprises qui sont des concurrents sur d'autres domaines il y a de la confidentialité “interne” à l'entreprise.

Typologie des politiques de sécurité

Définition

Chaque contexte et/ou organisation a ses propres besoins ainsi que ses propres “niveaux” de confidentialité, intégrité et disponibilité.

- Les politiques de sécurité militaire sont essentiellement centrées sur la confidentialité.
- Les politiques de sécurité commerciale (industrielle) sont essentiellement centrées sur l'intégrité et la disponibilité.

Remarque

Cette distinction paraît moins d'actualité !
Pour les militaires, il y a beaucoup d'applications qui réclament de l'intégrité (pour le renseignement) et de la disponibilité (des systèmes).
Le carnet de commande Apple chez TSMC ou Samsung n'est pas publique, de plus dans des entreprises qui sont des concurrents sur d'autres domaines il y a de la confidentialité “interne” à l'entreprise.

Notion de confiance...

La confiance au coeur de la sécurité

La sécurité repose sur les notions évoquées ci-dessus, mais elle repose aussi sur l'hypothèse que les choses sont correctes et que la chaine de “confiance” est conservée. Reprenons l'exemple donné par Matt Bishop dans son livre.

Intsallation d'une “correction du système d'exploitation”

La correction logicielle est-elle celle qui a été émise par le constructeur ?
La correction logicielle est-elle correcte ?
(Elle a été réalisée dans l'urgence par le constructeur, ne génère-t-elle pas un nouveau trou de sécurité dans le système, qui sera corrigée sous 48 h ?)
N'y a-t-il pas une incohérence entre les corrections installées sur le système ? (Ont elles été toutes installées ?)
La correction sera-t-elle bien installée ?

Notion de confiance...

La confiance au coeur de la sécurité

La sécurité repose sur les notions évoquées ci-dessus, mais elle repose aussi sur l'hypothèse que les choses sont correctes et que la chaine de “confiance” est conservée. Reprenons l'exemple donné par Matt Bishop dans son livre.

Intsallation d'une “correction du système d'exploitation”

La correction logicielle est-elle celle qui a été émise par le constructeur ?
La correction logicielle est-elle correcte ?
(Elle a été réalisée dans l'urgence par le constructeur, ne génère-t-elle pas un nouveau trou de sécurité dans le système, qui sera corrigée sous 48 h ?)
N'y a-t-il pas une incohérence entre les corrections installées sur le système ? (Ont elles été toutes installées ?)
La correction sera-t-elle bien installée ?

le cnam

Typologie des contrôles d'accès

Une politique de sécurité met en oeuvre plusieurs types de contrôle d'accès. Ce deux derniers peuvent être utilisés seuls ou combinés.

Définition : Mécanisme discrétionnaire (ou DAC pour Discretionary Access Control)

Si un utilisateur individuel peut déterminer quels sont les personnes qui peuvent accéder ou pas à un objet, on parle d'un mécanisme discrétionnaire.

Définition : Mécanisme obligatoire (ou MAC pour Mandatory Access Control)

Quand le système contrôle l'accès aux objets et qu'un utilisateur individuel ne peut modifier les droits sur un objet, on parle d'un mécanisme obligatoire.

Typologie des contrôles d'accès

Une politique de sécurité met en oeuvre plusieurs types de contrôle d'accès. Ce deux derniers peuvent être utilisés seuls ou combinés.

Définition : Mécanisme discrétionnaire (ou DAC pour Discretionary Access Control)

Si un utilisateur individuel peut déterminer quels sont les personnes qui peuvent accéder ou pas à un objet, on parle d'un mécanisme discrétionnaire.

Définition : Mécanisme obligatoire (ou MAC pour Mandatory Access Control)

Quand le système contrôle l'accès aux objets et qu'un utilisateur individuel ne peut modifier les droits sur un objet, on parle d'un mécanisme obligatoire.

le cnam

Politique de sécurité

- Politique orientée confidentialité
  - Bell LaPadula Model
- Politique orientée intégrité
  - Biba
- Autre modèle
  - Chinese Wall

le cnam

Bell LaPadula

- Notion de "clearance" (dédouanement) qui représente la sensibilité liée aux informations. Un objet a une classification, toutes les informations sont classifiées dans un ordre strict. Un sujet a un niveau de sécurité.

Model	Objet (exemple avec des données)	Sujet
Top Secret	Pin Code, Pwd	Owner
Secret	Mail	Friends/Colleagues
Confidential	Log Files	Admin
Unclassified	Cnam Phone List	All

- De manière plus formelle...

le cnam

Bell LaPadula

Model	Objet (exemple avec des données)	Sujet
Top Secret	Personal Files	Alice
Secret	Mail	Bob
Confidential	Log Files	Cyndy
Unclassified	Cnam Phone List	All

Soit L(S) le niveau de sécurité (clearance) d'un sujet S. Soit L(O)=$l_o$le niveau de classification d'un objet O. Pour toute classification de sécurité $l_i, i = 0, \ldots, k-1,\ l_i = l_{i+1}$.

Condition de sécurité simple initiale

S peut lire O si et seulement si $l_0 \leq l_s$ et S a le droit discrétionaire de lire O.

Limites !

Cyndy ne peut pas lire les Personal Files, mais Bob et Cyndy peuvent lire les Log Files. Alice peut copier le contenu de Personal Files dans Log Files, Alice peut donner le droit de lire à Cyndy...

Bell LaPadula

Model	Objet (exemple avec des données)	Sujet
Top Secret	Personal Files	Alice
Secret	Mail	Bob
Confidential	Log Files	Cyndy
Unclassified	Cnam Phone List	All

Soit L(S) le niveau de sécurité (clearance) d'un sujet S. Soit L(O)=$l_o$le niveau de classification d'un objet O. Pour toute classification de sécurité $l_i, i = 0, \ldots, k-1,\ l_i = l_{i+1}$.

Condition de sécurité simple initiale

S peut lire O si et seulement si $l_0 \leq l_s$ et S a le droit discrétionaire de lire O.

Limites !

Cyndy ne peut pas lire les Personal Files, mais Bob et Cyndy peuvent lire les Log Files. Alice peut copier le contenu de Personal Files dans Log Files, Alice peut donner le droit de lire à Cyndy...

Bell LaPadula

Model	Objet (exemple avec des données)	Sujet
Top Secret	Personal Files	Alice
Secret	Mail	Bob
Confidential	Log Files	Cyndy
Unclassified	Cnam Phone List	All

Soit L(S) le niveau de sécurité (clearance) d'un sujet S. Soit L(O)=$l_o$le niveau de classification d'un objet O. Pour toute classification de sécurité $l_i, i = 0, \ldots, k-1,\ l_i = l_{i+1}$.

Condition de sécurité simple initiale

S peut lire O si et seulement si $l_0 \leq l_s$ et S a le droit discrétionaire de lire O.

Limites !

Cyndy ne peut pas lire les Personal Files, mais Bob et Cyndy peuvent lire les Log Files. Alice peut copier le contenu de Personal Files dans Log Files, Alice peut donner le droit de lire à Cyndy...

Bell LaPadula

Soit L(S) le niveau de sécurité (clearance) d'un sujet S. Soit L(O)=$l_o$le niveau de classification d'un objet O. Pour toute classification de sécurité $l_i, i = 0, \ldots, k-1,\ l_i = l_{i+1}$.

Condition de sécurité simple initiale

S peut lire O si et seulement si $l_0 \leq l_s$ et S a le droit discrétionaire de lire O.

Propriété * de sécurité initiale

S peut écrire O si et seulement si $l_s \leq l_o$ et S a le droit discrétionaire d'accéder à O.
On dit aussi que dans le cas de l'écriture "l'objet doit dominer le sujet" et dans le cas de la lecture "le sujet domine l'objet".

Bell LaPadula

Soit L(S) le niveau de sécurité (clearance) d'un sujet S. Soit L(O)=$l_o$le niveau de classification d'un objet O. Pour toute classification de sécurité $l_i, i = 0,...,k-1$, $l_i = l_{i+1}$.

Condition de sécurité simple initiale

S peut lire O si et seulement si $l_0 \leq l_s$ et S a le droit discrétionaire de lire O.

Propriété * de sécurité initiale

S peut écrire O si et seulement si $l_s \leq l_o$ et S a le droit discrétionaire d'accéder à O.
On dit aussi que dans le cas de l'écriture "l'objet doit dominer le sujet" et dans le cas de la lecture "le sujet domine l'objet".

Bell LaPadula

Théorème

*Soit un système Σ, l'état initial σ_0 et T l'ensemble des transformations. Si toute toute transition σ_i préserve la condition de sécurité simple initiale et la propriété * de sécurité initiale alors tous les états σ_i, $i \geq 0$ sont sûrs.*

Bell LaPadula

Le principe de *tranquilité*.
Le niveau de sécurité d'un sujet ou d'un objet ne change pas au fil du temps.
Donner un exemple sur le tableau suivant du changement de statut d'un objet et d'un sujet. Quelles conséquences ?

Model	Objet (exemple avec des données)	Sujet
Top Secret	Personal Files	Alice
Secret	Mail	Bob
Confidential	Log Files	Cyndy
Unclassified	Cnam Phone List	All

Bell LaPadula (La contreverse)

La contreverse à propos de Bell-LaPadula.
En 1985 Mc Lean :

- La *valeur* du théorème est trop surévaluée
- Il est difficile d'imaginer une situtaion *pratique* qui soit représentable

Mc Lean inroduit une nouvelle propriété†, où pour écrire le sujet doit dominer l'objet et pour lire le sujet doit aussi dominer l'objet. (C'est le contraire de la propriété *.
for writing, subject dominates object ; for reading, subject also dominates object Differs from *-property in that the mandatory condition for writing is reversed For *-property, it's object dominates subject
Une partie du débat est *théorique*.

- La modélisation
  - on part de l'abstraction de la réalité pour arriver à des propriétés générales (Bell-LaPadula)
  - on part d'axiomes , on construit des modèles à partir de ces axiomes et on étudie les effets (McLean)

Bell LaPadula (Conclusion)

- Bell LaPadula restreint les flots de données
- Bell LaPadula modélise la sécurité multi-niveau

Politique de sécurité pour l'intégrité

Objectifs

Préserver l'intégrité des données manipulées par le système.
Lipner énonce 5 exigences pour préserver l'intégrité d'un système :

1. Les utilisateurs ne peuvent pas écrire leurs propres programmes et doivent seulement utiliser ceux des services de production des programmes.
2. Les services de production des programmes ne peuvent utiliser que des données de tests, si ils veulent utiliser des données de production, cela ce fait à travers un processus spécifique et sur le système de developement
3. Un processus particulier doit être mis en place pour installer de nouveaux programmes de production pour les utilisateurs.
4. Le point 3 doit être auditable.
5. Les auditeurs et le management doivent avoir accès au système et aux enregistrements (log) qui ont été générés par le process.

Politique de sécurité pour l'intégrité

Les principes associées

Séparation des rôles

En cas de besoin de réaliser plusieurs fonctions sensibles, celles ci ne doivent pas être réalisées par la même personne.
Dans le cas évoqué au dessus, un nouveau programme est produit par les équipes de production. Les équipes de geston du système doivent vérifier que celui-ci est correct puis l'installer. Dans ce cas un programme corrompu ne sera pas installé à moins qu'il y est collusion entre les acteurs.

...

Politique de sécurité pour l'intégrité

Les principes associées

Séparation des functions

Les développeurs développement sur des jeux de données de test et pas de production, ils ne peuvent et doivent interférer (agir) sur des données de production

Capacité d'audit

Pour l'intégrité, il est importat de pouvoir reconstituer le système et/ou de déterminer les actions responsables d'une situation ou d'un fait. Les logs permettent de tenir la liste des fonctions à réaliser pour obtenir une situation données à partir d'une situation connues.

Politique de sécurité pour l'intégrité

Les principes associées

Séparation des functions

Les développeurs développement sur des jeux de données de test et pas de production, ils ne peuvent et doivent interférer (agir) sur des données de production

Capacité d'audit

Pour l'intégrité, il est importat de pouvoir reconstituer le système et/ou de déterminer les actions responsables d'une situation ou d'un fait. Les logs permettent de tenir la liste des fonctions à réaliser pour obtenir une situation données à partir d'une situation connues.

Politique de sécurité pour l'intégrité

À partir de Biba, K. J., "Integrity Considerations for Secure Computer Systems," ESD-TR- 76-372, USAF Electronic Systems Division, Bedford, Mass. (Apr. 1977).
Dans ce papier il étudie et propose une formalisation de la propriété d'intégrité.

Notations

S un ensemble de sujet s.
O un ensemble d'objet o.
I un iveau d'intégrité i attaché à un sujet ou à un objet. Les niveaux sont *ordonnés*.
La relation $k < I$ ($k \leq I$) $\subseteq I \times I$, capte le fait que I domine k (ou domine et est égale à k).
Le $min : I \times I \longrightarrow I$ fournit le plus petit élément.
La fonction $i : S \cup O \longrightarrow I$ retourne la valeur entière du niveau d'intégrité du sujet ou d'un objet.
La relation $\underline{r}$ (resp. $\underline{w}$, $\underline{x}$) $r \subseteq S \times O \longrightarrow$ définit la capacité du sujet s lire (resp. écrire, exécuter) sur l'objet o.

Politique de sécurité pour l'intégrité

À partir de Biba, K. J., "Integrity Considerations for Secure Computer Systems," ESD-TR- 76-372, USAF Electronic Systems Division, Bedford, Mass. (Apr. 1977).
Dans ce papier il étudie et propose une formalisation de la propriété d'intégrité.

Notations

S un ensemble de sujet s.
O un ensemble d'objet o.
I un iveau d'intégrité i attaché à un sujet ou à un objet. Les niveaux sont *ordonnés*.
La relation $k < I$ ($k \leq I$) $\subseteq I \times I$, capte le fait que I domine k (ou domine et est égale à k).
Le $min : I \times I \longrightarrow I$ fournit le plus petit élément.
La fonction $i : S \cup O \longrightarrow I$ retourne la valeur entière du niveau d'intégrité du sujet ou d'un objet.
La relation $\underline{r}$ (resp. $\underline{w}$, $\underline{x}$) $r \subseteq S \times O \longrightarrow$ définit la capacité du sujet s lire (resp. écrire, exécuter) sur l'objet o.

Politique de sécurité pour l'intégrité

Intuitivement : une donnée ou un programme sensible a un haut niveau d'intégrité.
De manière sous jacentes il y a un notion de niveau de confiance.

Transfert d'information

Un transfert d'information est une séquence d'objet o_1, ..., o_{n+1}, à laquelle correspond une suite de sujet s_i, ..., s_n, tel que $s_i \ \underline{r} \ o_i$ et $s_i \ \underline{w} \ o_{i+1}$ pour tout i, $1 \leq i \leq n$.

Intuitivement : les données de l'objet o_i sont transmises dans l'objet o_{n+1} par la suite de lecture/écriture.

Politique de sécurité pour l'intégrité

Intuitivement : une donnée ou un programme sensible a un haut niveau d'intégrité.
De manière sous jacentes il y a un notion de niveau de confiance.

Transfert d'information

Un transfert d'information est une séquence d'objet o_1, ..., o_{n+1}, à laquelle correspond une suite de sujet s_i, ..., s_n, tel que s_i r o_i et s_i w o_{i+1} pour tout i, $1 \leq i \leq n$.

Intuitivement : les données de l'objet o_i sont transmises dans l'objet o_{n+1} par la suite de lecture/écriture.

Politique de sécurité pour l'intégrité

Intuitivement : une donnée ou un programme sensible a un haut niveau d'intégrité.
De manière sous jacentes il y a un notion de niveau de confiance.

Transfert d'information

Un transfert d'information est une séquence d'objet o_1, ..., o_{n+1}, à laquelle correspond une suite de sujet s_i, ..., s_n, tel que s_i r o_i et s_i w o_{i+1} pour tout i, $1 \leq i \leq n$.

Intuitivement : les données de l'objet o_i sont transmises dans l'objet o_{n+1} par la suite de lecture/écriture.

le cnam

Politique de sécurité pour l'intégrité

Politique à faible marquage, quand un sujet peut accéder à un objet, alors le niveau d'intégrité du sujet devient le niveau d'intégrité le plus faible de l'objet ou du sujet considérés.

Définition

1. $s \in S$ peut écrire sur $o \in O$ ssi $i(o) \leq i(s)$.
2. Si $s \in S$ lit $o \in O$, *alors* $i'(s) = min\ \{i(s), i(o)\}$ ou $i'(s)$ est le niveau d'intégrité du sujet s après la lecture.
3. $s_i \in S$ *peut exécuter* $s_{i+1} \in S$ *ssi* $i(s_{i+1}) \leq i(s_i)$.

Le 1 signifie que s peut écrire sur un objet o si il a un niveau d'intégrité haut. (Il "domine l'objet"). À contrario, il ne pourra écrire sur un objet ayant une intégrité plus forte que lui.
Le 2 signifie que si un sujet lit un objet de plus faible niveau d'intégrité, alors il verra son niveau baisser au niveau de celui de l'objet.
Le 3 signifie qu'un sujet peut exécuter un autre sujet si il a un niveau supérieur.

Politique de sécurité pour l'intégrité

Politique à faible marquage, quand un sujet peut accéder à un objet, alors le niveau d'intégrité du sujet devient le niveau d'intégrité le plus faible de l'objet ou du sujet considérés.

Définition

1. $s \in S$ peut écrire sur $o \in O$ ssi $i(o) \leq i(s)$.
2. Si $s \in S$ lit $o \in O$, *alors* $i'(s) = min\ \{i(s), i(o)\}$ ou $i'(s)$ est le niveau d'intégrité du sujet s après la lecture.
3. $s_i \in S$ *peut exécuter* $s_{i+1} \in S$ *ssi* $i(s_{i+1}) \leq i(s_i)$.

Le 1 signifie que s peut écrire sur un objet o si il a un niveau d'intégrité haut. (Il "domine l'objet"). À contrario, il ne pourra écrire sur un objet ayant une intégrité plus forte que lui.
Le 2 signifie que si un sujet lit un objet de plus faible niveau d'intégrité, alors il verra son niveau baisser au niveau de celui de l'objet.
Le 3 signifie qu'un sujet peut exécuter un autre sujet si il a un niveau supérieur.

Politique de sécurité pour l'intégrité

Politique à faible marquage, quand un sujet peut accéder à un objet, alors le niveau d'intégrité du sujet devient le niveau d'intégrité le plus faible de l'objet ou du sujet considérés.

Définition

1. $s \in S$ peut écrire sur $o \in O$ ssi $i(o) \leq i(s)$.
2. Si $s \in S$ lit $o \in O$, *alors* $i'(s) = min\ \{i(s), i(o)\}$ ou $i'(s)$ est le niveau d'intégrité du sujet s après la lecture.
3. $s_i \in S$ *peut exécuter* $s_{i+1} \in S$ *ssi* $i(s_{i+1}) \leq i(s_i)$.

Le 1 signifie que s peut écrire sur un objet o si il a un niveau d'intégrité haut. (Il "domine l'objet"). À contrario, il ne pourra écrire sur un objet ayant une intégrité plus forte que lui.
Le 2 signifie que si un sujet lit un objet de plus faible niveau d'intégrité, alors il verra son niveau baisser au niveau de celui de l'objet.
Le 3 signifie qu'un sujet peut exécuter un autre sujet si il a un niveau supérieur.

Politique de sécurité pour l'intégrité

Théorème

Il y a un un chemin de transfert de données d'un objet $o_1 \in O$ *à un objet* $o_{n+1} \in O$, *alors l'application de la politique à faible marquage exige que* $i(o_{i+1}) \leq i(o_1)$ *pour* $1 \leq i \leq n$.

Démonstration.

Par la définition sur le transfert d'information, il existe une suite de sujet et d'objet t.q. s_j r o_j et s_j w o_{j+1} pour tout i, $1 \leq j \leq k$.
On a aussi (point 2 définition), $i(s_k) = min\ \{\ i(o_j)\ /\ 1 \leq j \leq k\ \}$ après k lectures.
La $n^{ème}$ écriture réussie, par le point 1 définition, $i(o_{n+1}) \leq i(s_n)$.
Par transitivité on a $i(o_{i+1}) \leq i(o_1)$. □

Politique de sécurité pour l'intégrité

Théorème

Il y a un un chemin de transfert de données d'un objet $o_1 \in O$ *à un objet* $o_{n+1} \in O$, *alors l'application de la politique à faible marquage exige que* $i(o_{i+1}) \leq i(o_1)$ *pour* $1 \leq i \leq n$.

Démonstration.

Par la définition sur le transfert d'information, il existe une suite de sujet et d'objet t.q. s_j r o_j et s_j w o_{j+1} pour tout i, $1 \leq j \leq k$.
On a aussi (point 2 définition), $i(s_k) = min\ \{\ i(o_j)\ /\ 1 \leq j \leq k\ \}$ après k lectures.
La $n^{ème}$ écriture réussie, par le point 1 définition, $i(o_{n+1}) \leq i(s_n)$.
Par transitivité on a $i(o_{i+1}) \leq i(o_1)$. □

Politique de sécurité pour l'intégrité

La politique décrite a des inconvénients...
Très vite le niveau des sujets va baisser au fil des lectures écritures.
On peut mettre la dégradation sur les objets mais dans ce cas aussi très vite ce sont les objets qui vont se retrouver avec des niveaux très bas !

le cnam

Politique de sécurité pour l'intégrité

Définition

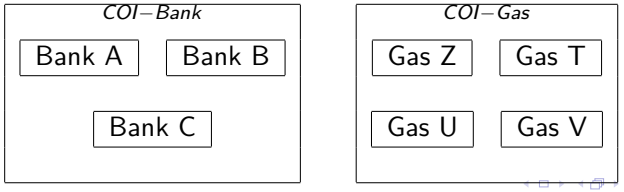
Le modèle de Biba.
1. $s \in S$ peut lire sur $o \in O$ ssi $i(s) \leq i(o)$.
2. $s \in S$ peut écrire sur $o \in O$ ssi $i(o) \leq i(s)$.
3. $s_i \in S$ *peut exécuter* $s_{i+1} \in S$ *ssi* $i(s_{i+1}) \leq i(s_i)$.

Le théorême reste vrai (changement dans la preuve).
Si la lecture et l'écriture sont autorisées alors $i(s) = i(o)$.

Chinese Wall

Introduit en 1989 by D. Brewer and M. Nash.

- Cette méthode gère la confidentialité et l'intégrité mais introduit la notion de conflit d'intérêt qui est plus requise en environnement commercial/industriel qu'en environnement militaire.
- Ce modèle est lié aux échanges en bourse et ou à la gestion de comptes en banque.
- On découpe le business en groupe d'intérêts COI (conflict of Interest).
- Dans un COI les entreprises sont en compétition. Un employé ne peut pas par exemple travailler que pour une entité par COI.
- Soit CD un ensemble d'objet se rapportant à une société



Chinese Wall

Il y a une notion de temporalité qui doit apparaître.

- On peut exprimer cette contrainte de la manière suivante :
- Soit PL (S) = l'ensemble des informations auxquelles à accéder le sujet s.

Définition

Première version
S peut lire un objet O ssi une de ces conditions est vraie :

- Il y un objet O' tel que S à accès à O' et CD(O) = CD(O')
- Pour tout objet O', O' $\in$ PL(S) $\Longrightarrow$ COI(O') $\neq$ COI(O)

L'état initial de PL(S) = Ø

Chinese Wall

Il y a une notion de temporalité qui doit apparaître.

- On peut exprimer cette contrainte de la manière suivante :
- Soit PL (S) = l'ensemble des informations auxquelles à accéder le sujet s.

Définition

Première version
S peut lire un objet O ssi une de ces conditions est vraie :

- Il y un objet O' tel que S à accès à O' et CD(O) = CD(O')
- Pour tout objet O', O' $\in$ PL(S) $\Longrightarrow$ COI(O') $\neq$ COI(O)

L'état initial de PL(S) = Ø

Chinese Wall

Les conséquences sont :

- Si un sujet a commencé à lire des objets d'un CD dans un COI, il ne peut plus obtenir de droit de lecture sur un autre CD de ce COI.
- Il est nécessaire d'avoir au moins autant de sujet que de CD dans les COI.

En fait, certaines données des entreprises deviennent publiques (bilan, (r)achats,...)

Définition

Deuxième version
S peut lire un objet O ssi une de ces conditions est vraie :

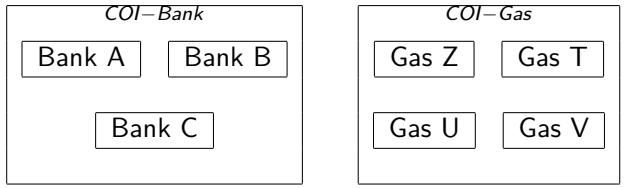
- Il y un objet O' tel que S à accès à O' et CD(O) = CD(O')
- Pour tout objet O', O' $\in$ PL(S) $\Longrightarrow$ COI(O') $\neq$ COI(O)
- O est un objet divulgué

L'état initial de PL(S) = Ø

Chinese Wall

Quels risques existent encore avec ces définitions ?

-



Supposons

- Alice peut lire CD(A), Bob peut lire CD (B)
- Alice et Bob peuvent lire CD(Z)
- Bob peut écrire dans CD(Z)
- ... indirectement Alice peut obtenir de l'information en provenance de CD(B) !

Chinese Wall

Les conséquences sont :

- Si un sujet a commencé à lire des objets d'un CD dans un COI, il ne peut plus obtenir de droit de lecture sur un autre CD de ce COI.
- Il est nécessaire d'avoir au moins autant de sujet que de CD dans les COI.

En fait, certaines données des entreprises deviennent publiques (bilan, (r)achats,...)

Définition

Deuxième version
S peut lire un objet O ssi une de ces conditions est vraie :

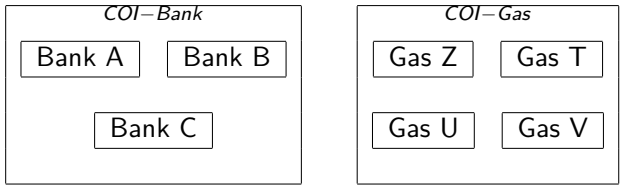
- Il y un objet O' tel que S à accès à O' et CD(O) = CD(O')
- Pour tout objet O', O' $\in$ PL(S) $\Longrightarrow$ COI(O') $\neq$ COI(O)
- O est un objet divulgué

L'état initial de PL(S) = Ø

Chinese Wall

Quels risques existent encore avec ces définitions ?

-



Supposons

- Alice peut lire CD(A), Bob peut lire CD (B)
- Alice et Bob peuvent lire CD(Z)
- Bob peut écrire dans CD(Z)
- ... indirectement Alice peut obtenir de l'information en provenance de CD(B) !

Chinese Wall

Définitions Propriété *

Un sujet S peut écrire dans un objet O ssi les deux conditions sont vraies :

- Le modèle permet à S de lire 0
- Pour tout objets O' non divulgués, S peut lire O' $\Longrightarrow$ CD(O') = CD(O)

Comparaison des différents modèles

Comparaison des approches

Dans Bell La Padula, il y a des labels de sécurité associés aux sujets.
Le model Chinese Wall prend en compte la notion des accès passés.

Exercices 1

On considère les niveaux d'habilitation H suivants : TOPSECRET, SECRET, CONFIDENTIEL et NON-CONFIDENTIEL.
On y ajoute la notion de catégorie (ou compartiment) notée C.
Par exemple NUC et ARM. Ces catégories forment un treillis ordonné comportant les éléments suivants : ϕ,$\{NUC\}$,$\{ARM\}$ *et* $\{NUC, ARM\}$.
Dans la suite de l'exercise on parlera de niveau de sécurité pour le couple constitué d'un niveau d'habilitation et d'une catégorie noté *(H, C)*.

Définition

Définition On dira qu'un niveau de sécurité (H, C) **domine** un niveau de sécurité (H', C') si et seulement $H' \leq H$ et $C' \subseteq C$.

Exercice 1 suite

Bob a son niveau de sécurité décrit par le couple $(SECRET, \{NUC\})$.
Soient les documents et leur son niveau de sécurité :

- Doc_A est classifié au niveau $(CONFIDENTIEL, \{NUC\})$
- Doc_B est classifié au niveau $(SECRET, \{NUC, ARM\})$
- Doc_C est classifié au niveau $(SECRET, \{NUC\})$

Pour l'exemple ci-dessus :

- Bob domine le Doc_A car $CONFIDENTIEL \leq SECRET$ et $\{NUC\} \subseteq \{NUC\}$
- Bob ne domine pas le Doc_B car $\{NUC, ARM\} \nsubseteq \{NUC\}$
- Bob domine le Doc_C car $SECRET \leq SECRET$ et $\{NUC\} \subseteq \{NUC\}$

Exercice 1 Question

Question 1 Quel intérêt voyez vous à introduire cette notion de « catégorie » ou « compartiment » dans le modèle ?

Question 2 Soient les niveaux d'habilitation H suivants : TOPSECRET, SECRET, CONFIDENTIEL et NON-CONFIDENTIEL.
Soient les catégories suivantes : A, B et C. Énumérer les éléments du treillis des catégories.

Question 3 Pour les utilisateurs et documents suivants précisez et justifiez les utilisateurs qui dominent les documents :

- Vincent avec $(TOPSECRET, \{A, C\})$ comme niveau de sécurité et le document $\text{Doc}_1(SECRET, \{B, C\})$
- François avec $(CONFIDENTIEL, \{C\})$ comme niveau de sécurité et le document $\text{Doc}_2(SECRET, \{C\})$
- Paul avec $(SECRET, \{C\})$ comme niveau de sécurité et le document $\text{Doc}_3(SECRET, \{B, C\})$
- Jacques avec $(TOPSECRET, \{A, C\})$ comme niveau de sécurité et le document $\text{Doc}_4(SECRET, \{A\})$
- Jean avec $(NON - CONFIDENTIEL, \{\phi\})$ comme niveau de sécurité et le document $\text{Doc}_5(SECRET, \{B\})$

Exercices 2

Exercices 2

Développer et proposer un modèle du type Chinese Wall qui puisse représenter/supporter un modèle du type Bell La Padula ?