Contrôles d'accès basés sur treillis et modèles de sécurité

Franck Jeannot

U638, Montréal, Canada, Décembre 2019 : v1.0 ; Dernière version : Janvier 2021 : v1.2

Abstract

Lattice-Based access controls (**LBAC**) is a general category for **NDAC** (nondiscretionary access controls). In this category, subjects under lattice-based access controls are assigned **positions** in a lattice (either a **security label** or a **clasification**). « ***Subjects*** *can access only those* ***objects*** *that fall into the range between the* ***LUB*** *(Least Upper Bound) (the nearest security label or classification higher than their lattice position) and the* ***GLB*** *Greatest/-highest Lower Bound (the nearest security label or classification lower than their lattice position) of the labels or clasifications for their lattice position* » [1].

Keywords: DAC, Denning, ensemble ordonné, join and meet, Lattice, Hasse, hiérarchie, LBAC, MAC, NDAC, ordre, partially ordered set, poset, précédence, treillis, Sandhu

1. Treillis et sécurité

Les *contrôles d'accès basés sur* ***treillis*** ou **LBAC** sont utilisés pour définir des niveaux de sécurité des ***objets*** et des ***sujets*** via *des* ***labels*** *ou* ***étiquettes de sécurité*** en renforçant un *flux d'information unidirectionnel* [2]. Quand un label est sur un *objet*, on parle de *classification de sécurité*, alors que si le label est sur un *sujet*, on parle d'*habilitation de sécurité* (*security clearance*). Les étiquettes de sécurité forment un *treillis* tel que l'élément le plus haut du treillis est le plus sensible [3].

Les contrôles LBAC peuvent être utilisés pour la confidentialité, l'intégrité, ces 2 composantes ou bien des aggrégations diverses de polices comme le modèle « Muraille de chine ». Le modèle de Bell-LaPadula (confidentialité) [4] [5] décrit un jeu de règles qui proscrit tout flux d'information d'un haut niveau vers un plus bas niveau. Une appellation **LaBAC** ***Label****-Based Access Control* [6] existe aussi mais n'est pas développée ici.

1. CISSP Study guide, p. 324, Stewart (2015), [1]
2. Sandhu (1998), p. 35/50 de [2]
3. Sabri (2009), p. 5 de [3]

Les **LBAC** sont essentiellement des *Contrôles d'Accès Obligatoires* ou **MAC** (*Mandatory Access Controls*) qui sont *typiquement ajoutés en plus* [4] de classiques contrôles d'accès discrétionnaires **DAC**. Dans le domaine des contrôles d'accès de sécurité, on aura alors :

— *des niveaux de sécurité* **H** avec des classifications linéaires $\leq$

— des *catégories* **C** tels que les noms de projet, divisions de l'entreprise, etc.

— des *étiquettes de sécurité* qui sont des paires (h,c) où $h \in H$ et $c \subseteq C$

On définit une *étiquette de sécurité* par la paire (*niveau de sécurité* **H**, *ensemble de catégories* **C**).

2. Treillis et définitions

On retrouve diverses définitions dans la littérature, il en est repris plus bas des éléments importants. Les treillis ont des connexions avec la ***théorie des graphes*** [8].

Définition simplifiée. On appelle ***treillis*** un ensemble non vide et *partiellement ordonné* (4) dans lequel toute partie finie admet une **borne inférieure** et une **borne supérieure** [5]. Un poset (de l'anglais partially ordered set, en français "ensemble partiellement ordonné") formalise la notion intuitive d'ordre ou d'arrangement entre les éléments d'un ensemble. Un **poset** est un ensemble muni d'une relation d'ordre qui indique que pour certains couples d'éléments, l'un est plus petit que l'autre [6].

2.1. *Diagramme saggittal et Diagramme de Hasse*

Un *diagramme **saggital*** sert à représenter **une relation d'un ensemble fini vers un ensemble fini** dans lequel chaque couple est représenté par une **flèche**. Un *diagramme de **Hasse*** [7], est une représentation visuelle d'un **ordre fini**, c'est une version *simplifiée* [8] d'un diagramme *saggital* [9] [10] et **souvent utilisé pour représenter les treillis**.

2.2. *Opérateurs binaires Join $\vee$ et meet $\wedge$*

En mathématiques, spécifiquement dans la *théorie des ordres*, les notions d'opérateurs ***join*** et ***meet*** [8] d'un sous-ensemble S d'un ordre partiel P sont respectivement les **supremum** de S , noté $\vee S$ et l'**infimum** de S noté $\wedge S$.

4. Sandhu (1994), [7]
5. Wikipedia [9]
6. http://dictionnaire.sensagent.leparisien.fr/Poset/fr-fr/
7. Du mathématicien allemand Helmut **Hasse**
8. Voir Labourel p7/68 [10]
9. Voir pp 17-18 de [11]
10. Le mot « sagittal » vient du mot latin *sagitta* qui veut dire « flèche », [12]

Selon le mathématicien Gian-Carlo Rota [13] : « *Lattices are partially ordered sets in which least upper bounds and greatest lower bounds of any two elements exist.* ***Dedekind*** *[14] discovered that this property may be axiomatized by identities.* ***A lattice is a set on which two operations are defined, called join and meet*** *and denoted by* $\vee$ *and* $\wedge$ *which satisfy the idempotent, commutative and associative laws, as well as the absorption laws :* »

$$a \vee (b \wedge a) = a$$
$$a \wedge (b \vee a) = a$$

Exemple plus bas d'un diagramme de **Hasse** qui décrit un poset a 4 éléments : a,b, le **join** de a et b ($a \vee b$) ou **supremum ou least upper bound** et le **meet** de a et b ($a \wedge b$) ou **infimum ou great lower bound** [11]. Ici chaque paire dans ce poset à a la fois un meet et un join et donc peut être classée comme un **treillis**.

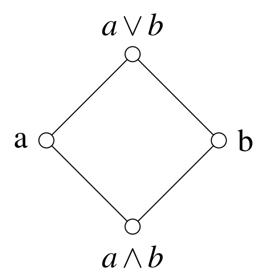

Figure (1) – Diagramme de ***Hasse*** *qui décrit un poset a 4 éléments*

Définition algébrique. [16] Un ensemble ordonné L est appelé un ***treillis*** si deux opérations binaires, **meet** et **join**, qui assignent à toute paire a, b des éléments de L, un élément unique $a \wedge b$ (*meet* de a et b) et un élément $a \vee b$ (join de a et b) de telle manière que les axiomes suvants du treillis soient satisfait. On définit a, b et $c \in L$. Alors :

$$\begin{array}{ll} L1 : (a \wedge b) \wedge c = a \wedge (b \wedge c), & L2 : (a \vee b) \vee c = a \vee (b \vee c) \\ L3 : a \wedge b = b \wedge a & L4 : a \vee b = b \vee a \\ L5 : a \wedge (a \vee b) = a & L6 : a \vee (a \wedge b) = a \end{array}$$

L1-L2 : loi associative (*associative law*) ; L3-L4 : loi commutative (*commutative law*) ; L5-L6 : loi d'absorption (*absorption law*) [12] Si L est un treillis, alors $a \wedge a = a$ et $a \vee a = a$ pour tous les a de L.

11. p. 33 de [15]
12. Paragraphe 14.8 LATTICES, page 346 de [17]

3. Treillis et origines

Les notions de *treillis* ont été d'abord introduites par George Boole (1824) puis Ernst Schröder en 1890 [16] [18]. Après cela, les travaux de P.G. Dirichlet (1894) [19] [20], ont été réutilisé en 1897, par Richard **Dedekind** qui fut crédité de la découverte des *treillis distributifs et modulaires*. En 1920, le mathématicien Norvégien Thoralf Albert Skolem apporta des éléments sur la théorie des treillis (*Gruppenkalkul*) [21]. Sur ces bases, dans les années 1930, Garrett **Birkhoff** fit de larges contributions à ce qui fut finalement qualifiée alors comme la *Théorie des treillis* [22] [23] [24]. Dans les années 1970, Bell, Biba, LaPadula, **Denning** [25] ont avancé la recherche dans le domaine des LBAC. Par la suite, nombre de ces modèles ont été implémentés, essentiellement en applications militaires. Par la suite **Sandhu** [26] en 1993 a complété la formalisation des LBAC. Bien que la théorie des treillis ait traversé différentes étapes de développement avec des approches et des attentes changeantes, ce domaine a considérablement augmenté chaque décennie depuis sa naissance [13] [27].

4. Ensembles totalement et partiellement ordonnés

4.1. Hiérarchie et précédence

Si on considère un ensemble P : avoir une ***hiérarchie*** sur P permet de définir une relation de **précédence** sur P : p est une relation avec q si p précède q dans la hiérarchie [10].

4.2. Propriétés de la précédence

— **antisymétrique** : si p et q sont différents et si p précède q alors q ne peut pas précéder p
— **transitive** : si p précède q et p précède r alors p précède r
— **réflexive** : $p \leq p$

4.3. ordre

Une relation **réflexive, antisymétrique et transitive** s'appelle une **relation d'ordre**. Un ensemble muni d'une **relation d'ordre** est un **ensemble ordonné**.

Autre Formalisation. Une relation R sur un ensemble A est appelée *ordre partiel* si elle est réflexive, anti-symétrique et transitive. Un ensemble A avec une relation d'ordre partiel R est appelé un ensemble partiellement ordonné ou *poset*. Ce poset est noté (S,R) [13].

13. Trad. libre de [28]

— Les relations $\leq$ et $\geq$ sur $\mathbb{N}$ sont des relations d'ordre
— Les relations $<$ et $>$ sur sur $\mathbb{N}$ n'en sont pas
— sur $\mathbb{N}^*$, la relation a divise b, notée $a|b$ est une relation d'ordre (a divise b s'il existe $k \in \mathbb{N}^*$ tel que $b = ka$). Par exemple, $3|24$.
— Relations d'ordre fréquentes : $\leq, \geq, \preceq, \succeq, \sqsubseteq, \sqsupseteq, \subseteq, \supseteq, |$ etc. Une notation générale est : $\ll$ et $\gg$.

4.4. Vocabulaire conventionnel d'une relation d'ordre

Si $x \ll y$, on dit que x est un **minorant** de y (x **minore** y) et y est un **majorant** de x (y **majore** x).

4.5. Poset

La notion d'« ensemble partiellement ordonné », de l'anglais *poset* [29], *partially ordered set* a été utilisée par **Birkhoff** dans son livre *Lattice theory* (1940) [22] [30]. C'est un ensemble muni d'une ***relation d'ordre*** [14]. Un **poset** $(P, \leq)$ est un ensemble P avec une relation $\leq$, appelée *ordre partiel*, tel que [15] :
— Pour tous les $p \in P$, on a $p \leq p$ (réflexivité)
— Pour tous les $p, q \in P$, si $p \leq q$ et $q \leq p$ alors $p = q$ (antisymétrie)
— Pour tous les $p, q, r \in P$, si $p \leq q$ et $q \leq r$ alors $p \leq r$ (transitivité)
On dit que p et q sont **comparables** si $p < q$ ou $p > q$, et ils sont **incomparables** autrement. On dit que q **couvre** p si $q > p$ et qu'il n'y a pas de $r \in P$ tel que $q > r > p$. Quand q **couvre** p, on écrit $q \gtrdot p$.
Pour pointer le fait qu'un ordre n'est pas **total** on dit qu'il s'agit d'un *ordre **partiel*** : certains éléments sont incomparables dans un tel ordre. Un ensemble **totalement** ordonné est un ensemble muni d'une relation d'ordre **total**.

Poset : autre formulation. [20] Un poset est un système $\mathscr{P} = (P, \leq)$ où P est non vide et $\leq$ est une relation binaire sur P satisfaisant pour tous les $x, y, z \in P$:

(1) $x \leq x$,	(réflexivité)
(2) si $x \leq y$ et $y \leq x$, alors $x = y$,	(antisymétrie)
(3) si $x \leq y$ et $y \leq z$, alors $x \leq z$.	(transitivité)

Par définition un treillis est un poset, cependant un poset n'est pas nécessairement un treillis.

14. relation binaire dans cet ensemble qui permet de comparer ses éléments entre eux de manière cohérente
15. on parle des 3 axiomes de réflexivité, anti-symétrie, transitivité

5. Polices de flux d'informations

Les stratégies de flux d'informations concernent le flux des informations d'une classe de sécurité à une autre. Dans un système, les informations circulent réellement d'un objet à un autre. Des exemples typiques d'objets sont les fichiers et les répertoires d'un système d'exploitation, ainsi que les relations et les *nuplets* dans un système de base de données [26].

5.1. Diagramme de Hasse avec 3 catégories

Le *modèle de contrôle d'accès basé sur treillis* plus bas (fig. 2) est un exemple de *Diagramme de Hasse*, selon (Ravi S. Sandhu, 1993) [26] qui montre un treillis d'une police avec 3 catégories **A,B,C** et qui peuvent dénoter des catégories comme "salaire", "medical" et "education". Au plus haut niveau d'accès on trouve la boîte **A,B,C**. Un **sujet** à ce niveau, a accès à tous les **objets** du treillis (voir aussi p. 81 de (Eric Conrad, 2011) [31]). Dans le second tiers du treillis, on observe que chaque objet a une limite distincte haute et basse. Par exemple si un sujet a accès à l'objet **A,C**, les seuls objets visibles dans le treillis sont les objets **A** et C, qui sont ses deux **GLB** (Greatest Lower Bound). Dans ce cas, le sujet ne pourrait avoir par exemple visibilité sur l'objet **B**.

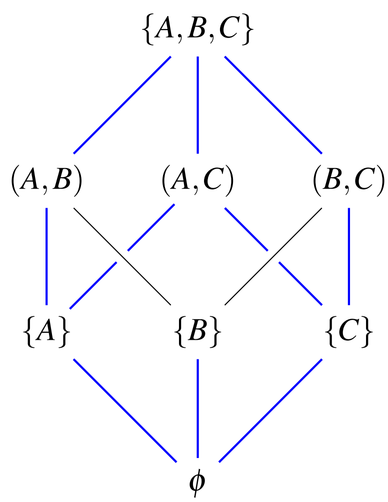

Figure (2) – Diagramme de Hasse avec 3 catégories A,B,C ; selon Sandhu-1993

5.2. Exemple d'accès à des ensembles de données

Dans (Meadows, 1990) (p. 3 de [32]) est donné un exemple de base de données qui se compose de six ensembles : A, B, C, D, E et F.

A, B, D et F ne sont pas classés (U=Unclassified), tandis que C et E sont (S) Secrets. Les agrégats exceptés sont B, D, qui est étiqueté Secret. Enfin A, B, C et C, E, qui sont (TS) Top Secret :

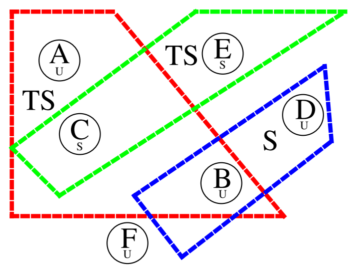

Figure (3) – Ensemble de données avec éléments de classifications

Au final un modèle d'accès basé sur treillis est construit (ref p. 6 de [32]))

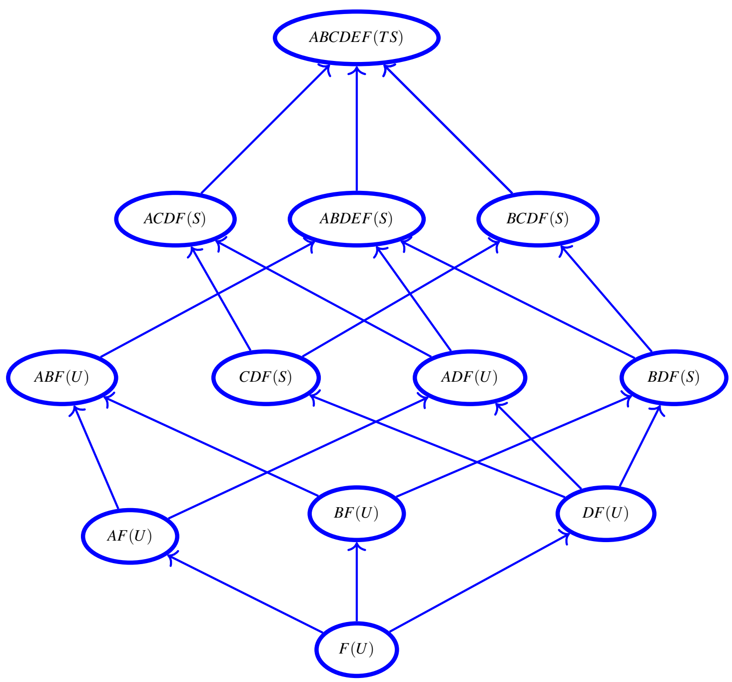

Figure (4) – Modèle d'accès basé sur Treillis

Références

[1] Stewart, J.M. and Chapple, M. and Gibson, D. and Seidl, D., CISSP (ISC)2 Certified Information Systems Security Professional Official Study Guide, 7th Edition, SYBEX Inc., Alameda, CA, USA, 2015.

[2] Ravi S. Sandhu, Role-based access control1, Vol. 46 of Advances in Computers, Elsevier, 1998, pp. 237 – 286. doi:https://doi.org/10.1016/S0065-2458(08)60206-5.
URL https://www.profsandhu.com/cs5323_s17/sandhu-1998.pdf

[3] Sabri, Khair Eddin and Khedri, Ridha and Jaskolka, Jason, Automated Verification of Information Flow in Agent-Based Systems, Tech. rep., McMaster University, Hamilton, ON, Canada (Jan. 2009).
URL http://www.cas.mcmaster.ca/cas/0reports/CAS-09-01-RK.pdf

[4] Bell, D Elliott and LaPadula, Leonard J, Secure computer systems: Mathematical foundations, Tech. rep., MITRE CORP BEDFORD MA, Massachusetts (1973).
URL http://www-personal.umich.edu/~cja/LPS12b/refs/belllapadula1.pdf

[5] Bell, D Elliott and LaPadula, Leonard J, Secure Computer Systems: Mathematical Foundations and Model, no. v. 1, Mitre Corporation, 1973.
URL https://books.google.ca/books?id=y_SNPAAACAAJ

[6] Biswas and Sandhu and Krishnan, Label-Based Access Control: An ABAC Model with Enumerated Authorization Policy.
URL https://profsandhu.com/cs6393_s16/prosun-abac16.pdf

[7] Ravi S. Sandhu and Pierangela. Samarati, Access control: principle and practice, IEEE Communications Magazine 32 (9) (1994) 40–48. doi:10.1109/35.312842.
URL https://www.profsandhu.com/cs5323_s18/SS-1994.pdf

[8] en.wikipedia.org, Join and meet.
URL https://en.wikipedia.org/wiki/Join_and_meet

[9] fr.wikipedia.org, Treillis (ensemble ordonné).
URL https://fr.wikipedia.org/wiki/Treillis_(ensemble_ordonn%C3%A9)

[10] Arnaud Labourel, Automates et circuits : Ordres, treillis et algèbre de boole.
URL http://pageperso.lif.univ-mrs.fr/~arnaud.labourel/AUTO/cours4.pdf

[11] V. di Giorgio, Application de l'algèbre de boole à l'étude des graphes, Mathématiques et Sciences humaines 36 (1971) 33–58.
URL http://www.numdam.org/article/MSH_1971__36__33_0.pdf

[12] SCOLAB netmath.ca, Diagramme sagittal.
URL https://lexique.netmath.ca/diagramme-sagittal/

[13] Rota, Gian-Carlo, The many lives of lattice theory 44 (11) (1997) 1440–1445.
URL http://www.ams.org/notices/199711/comm-rota.pdf

[14] plato.stanford.edu, Dedekind's contributions to the foundations of mathematics.
URL https://plato.stanford.edu/entries/dedekind-foundations

[15] Davey, B.A. and Priestley, H.A., Introduction to Lattices and Order, Second Edition, Cambridge University Press, 2002.
URL https://books.google.ca/books?id=BueMAgAAQBAJ

[16] Rintala, Richard Arne , Lattices.
URL https://digital.library.unt.edu/ark:/67531/metadc130744/m2/1/high_res_d/n_03398.pdf

[17] Lipschutz, S. and Lipson, M., Schaum's Outline of Discrete Mathematics, 3rd Ed., Schaum's Outline Series, McGraw-Hill Education, 2007.
URL https://books.google.ca/books?id=9KtFcFa81FcC

[18] G. Grätzer, Lattice Theory: Foundation, 2011. doi:10.1007/978-3-0348-0018-1.
URL https://www.researchgate.net/publication/258516222_Lattice_Theory_Foundation

[19] Lejeune-Dirichlet, Peter Gustav, Vorlesungen uber zahlentheorie (1894).
URL https://archive.org/details/vorlesungenberz02dirigoog/page/n14

[20] J.B Nation, Notes on lattice theory.
URL http://math.hawaii.edu/~jb/math618/Nation-LatticeTheory.pdf

[21] Skolem, Thoralf Albert, Solution of problems to decide whether a given statement in lattice theory (gruppenkalkul) is provable or nothttps://people.ucalgary.ca/~rzach/files/rzach/skolem1920.pdf - http://www.math.hawaii.edu/~jb/skolem2A.pdf (1920).

[22] Birkhoff, Garrett, Lattice theory, Colloquium publications, American Mathematical Society, Providence, RI, 1940.
URL https://cds.cern.ch/record/2264178

[23] Birkhoff, Garrett, Lattice Theory Revised Edition, second Edition, American Mathematical Society ; Colloquium Publications ; Volume XXV ; 311 p., 1948.
URL http://math.chapman.edu/~jipsen/summerschool/Birkhoff%201948%20Lattice%20Theory%20Revised%20Edition.pdfJ

[24] G. Birkhoff, Théorie et applications des treillis, Annales de l'institut Henri Poincaré 11 (5) (1949) 227–240.
URL http://www.numdam.org/article/AIHP_1949__11_5_227_0.pdf

[25] Denning, Dorothy E., A Lattice Model of Secure Information Flow, Commun. ACM 19 (5) (1976) 236–243. doi:10.1145/360051.360056.
URL http://doi.acm.org/10.1145/360051.360056

[26] R. S. Sandhu, Lattice-based access control models, Computer 26 (11) (1993) 9–19. doi:10.1109/2.241422.
URL http://www.winlab.rutgers.edu/~trappe/Courses/AdvSec05/access_control_lattice.pdf

[27] Bilová, Štěpánka, Lattice theory - its birth and life (2001).
URL https://dml.cz/bitstream/handle/10338.dmlcz/401261/DejinyMat_17-2001-1_31.pdf

[28] geeksforgeeks.org, Partial orders and lattices.
URL https://www.geeksforgeeks.org/mathematics-partial-orders-lattices

[29] Federico Ardila, Algebraic and geometric methods in enumerative combinatorics (2014).
URL https://arxiv.org/pdf/1409.2562.pdf

[30] G. Birkhoff, Lattice Theory, American Mathematical Society, Providence, 1967.

[31] Conrad, Eric, CISSP : Study Guide Eleventh Hour , Syngress ; Elsevier, 2011.

[32] Catherine Meadows, Extending the Brewer-Nash Model to a Multilevel Context, in : Proceedings. 1990 IEEE Computer Society Symposium on Research in Security and Privacy, 1990, pp. 95–102. doi:10.1109/RISP.1990.63842.