The theory of access control and flow control for data security:

From Partial orders to Lattices and back, a half-century trip

By Luigi Logrippo, luigi@uqo.ca
Université du Québec en Outaouais and University of Ottawa

(Position Paper: **feedback will be appreciated**)
Version 2025-05-28

Abstract: The multi-level Bell-La Padula model for secure data access and data flow control, formulated in the 1970's, was based on the theory of partial orders. Since then, another model, based on lattice theory, has prevailed. We present reasons why the partial order model is more appropriate.

Keywords: Data or information flow security, Bell-La Padula, Multi-level access control, and data flow control

This position (or discussion) paper is in the framework of the theory of data access control and data flow control for security in networks. In this theory, there are *entities* representing users, subjects, data objects such as databases and files, etc. *Access control rules* among entities define *Channels* among them, through which data can be directly transmitted. Through channels, data can be transmitted indirectly to other entities, and this possibility is represented by the transitive, reflexive closure of the Channel relation, the *CanFlow* relation. The CanFlow relation can contain symmetries, defining equivalence classes of entities that can get the same data, directly or indirectly. By taking classes of equivalent entities as units, symmetries are eliminated and the result is a partial order of equivalence classes. According to their position in the partial order, entities in networks can be assigned *security labels* that can be used by access control rules to define channels and data flows. Partial orders and labels define *Multi-level systems*, which establish data access and data flow control at the same time.

This theory, developed starting in the 1970's for operating system and database security, is still relevant today for data security in the Cloud, the IoT, and future-generation networks.

The first substantial research reports on the theory of data flow control were the well-known MITRE Corporation technical reports of David E. Bell and Len J. La Padula, produced over the years 1972-76. Reference [Bell, La Padula 1976] (BLP

henceforth) has an Appendix that presents a formal model, based on a partial order relation among labels. The report does not mention lattices and the example it provides (Fig. A1) shows a partial order of labels that is clearly not a lattice. The BLP model has been criticized as being too rigid, however access control matrices and access control methods define partial orders of labels, just as the BLP model does[Logrippo 2021].

In the same years, [Denning 1976] proposed that the partial order among security labels must be a *lattice*, which is *a partial order of labels where any two labels have unique joins and meets*. This is a strong requirement. A companion paper [Denning, Denning, Graham 1976] starts with the assertion "it has been shown that lattice-structured policies have properties which lead to simple and efficient enforcement mechanisms". It cites as evidence several papers, including some that do not mention lattice structures. It shows that non-lattice structured policies can be transformed into lattices "while preserving the validity of all flows", by a method involving the definition of new labels, not assigned to entities, we will call these *void* labels. Their main example (Fig. 1c) shows a partial order of labels, called *initial policy*, consistent with the definitions of [Logrippo 2021,2025]. It then shows that by adding four void labels, this partial order becomes a lattice. ***But, are the unique joins and meets, or the added void labels, useful for data security?*** Consider the following:

1. In many organizations, the required additional labels might contradict explicit security policies. For example, they include a label for entities that have access to all data, as well as a label for entities that have access to none [Denning, Denning, Graham 1976 and Sandhu 1993]. Also, for any two labels, there must be a label for entities that can receive data from both, in possible contradiction of conflict-of-interest policies.
2. As recognized in paper [Denning, Denning, Graham 1976], changes (or reconfigurations) in the network structure may be needed frequently: consider VANET networks, where many hundreds of entities can be involved, with many reconfigurations per second. The unnecessary algorithm for recovering the lattice-structure of the set of labels will have to be executed at each reconfiguration, with frequent addition of new void labels.
3. Since a subset of a lattice is not necessarily a lattice, the fact that a lattice data flow policy is implemented in an organization does not necessarily imply that it is implemented in all parts of the organization.

[Denning 1976] was a pioneering paper in the area of data flow control and had merits in addition to the proposal of the lattice model. According to Google Scholar, the paper has been cited almost 3,000 times.

Almost all subsequent research on data flow control for security has been influenced by the 'lattice' model, occasionally softened in terms of 'semi-lattices'. We find many explicit or implicit statements that a lattice structure of security labels is necessary for secure data flow control, without any real reasons. BLP and related MAC access control models were considered to be lattice models, and this was confirmed by D.E. Bell [Bell 1990]. But by using a more restricted mathematical model, the generality of the original BLP model is restricted. Many authors have noted that RBAC can define data flows that form partial orders but not lattices, hence the view that RBAC is more powerful than BLP or MAC. With the partial order original model for BLP, they have the same power [Logrippo 2025].

[Sandhu 1993] elaborates on the use and properties of the lattice model. It claims that the BLP model is lattice-based. It does express doubts about the lattice model, however. Sandhu writes that "although this article focuses on policies that satisfy Denning's axioms, there are legitimate information flow policies that do not satisfy these axioms". Also he shows an example illustrating that "in some situations it might be more appropriate to use partially ordered labels than to strive for a complete lattice".

Indeed, in support of these doubts, using a model based on elementary partial order theory, it can be proved that:

A. No void labels need to exist since labels can be assigned using a network's partial order structure: simply, each equivalence class of entities gets its unique label by a bottom-up construction, following the CanFlow relation that determines label inclusion. Thus, any network of communicating entities defines a partially ordered data flow of labels and entities, from equivalence classes that cannot receive from any others (thus having minimal labels and maximum integrity) to classes of entities that cannot send to any others (thus having maximal labels and maximum secrecy). In other words, *any network* defines a data security partial order of entities and associated labels, for secrecy and integrity [Logrippo 2021, Logrippo 2024].
B. Changes or reconfigurations in networks lead from partial orders to partial orders, and no void labels need to be added. If the partial order that a network defines does not conform to the security policies that the

network is supposed to implement, the network's partial order can be reconfigured to conform [Logrippo 2021].

C. Subsets of partial orders are partial orders. Any network and all its parts implement a data flow security policy by which the data flow is determined by label inclusion, and vice-versa.

This last concept is very intuitive: it can be explained in terms of the policy of an organization where entities have labels, stating what data they can know, and there is a channel (or data flow) from entity A to entity B iff the label of A is included in the label of B. The decision function of *all* access control and data flow control methods can be defined in terms of this policy.

Related claims

The author of this note and coauthors have shown that:

a) Labels calculated for partial orders of equivalence classes can be put in correspondence with network addresses (e.g. IP addresses), thus defining network routings that implement the CanFlow relationship [Stambouli, Logrippo 2024].
b) Data flow policies and access control policies are mutually convertible. Access control and data flow control for security can use the same mechanisms. All the commonly cited access control methods (DAC, partial order MAC, RBAC, ABAC).are 'complete' in the sense that they can define any CanFlow relation. As well, they can be mutually translated by using efficient algorithms [Logrippo 2025].
c) Several partially ordered data flows can be defined on the same set of entities, as is necessary for most applications (e.g. in e-commerce, there need to be data flows from the client to the company, and vice-versa). Entities participating in more than one flow have data conversion responsibilities [Stambouli, Logrippo 2024].
d) Efficient (i.e. polynomial) standard algorithms exist to support the partial order theory. Labels defined in this way can be calculated in linear time[Stambouli, Logrippo 2019].

Conclusion

With respect to partial order data flow theory, lattice data flow theory has limitations that are not compensated by any advantages apart from specific

applications where the existence of unique joins and meets may be necessary. We must go back to the partial order model proposed fifty years ago by Bell and La Padula, and explore the possibilities of partial order theory in its full generality and many specializations, in the recent application areas of data security in the IoT, the Cloud, mobile networks, etc.

As shown by the dates in the citations, this research area has advanced very slowly, but the door is now open to a unified theory of data and information protection, leading to developments in methods for privacy protection, secure routing and encryption in contemporary networks.

References (all papers can be found by simple search, see also https://www.site.uottawa.ca/~luigi/papers/99_luigi_papers_index.htm)

1. Bell, D.E., La Padula, L.J. (1976). Secure computer systems: unified exposition and Multics interpretation. MITRE Corp. ESD-TR-75-306
2. Bell, D. E. (1990). Lattices, policies, and implementations. In 13th National Computer Security Conference,165-171.
3. Denning, D. E. (1976). A lattice model of secure information flow. Communications of the ACM, 19(5), 236-243.
4. Denning, D. E., Denning, P. J., Graham, G. S. (1976). On the derivation of lattice structured information flow policies. Technical report, Purdue University.
5. Logrippo, L. (2021). Multi-level models for data security in networks and in the Internet of things. *Journal of Information Security and Applications*, *58*, 102778.
6. Logrippo, L. (2024). The order-theoretical foundation for data flow security. *arXiv preprint arXiv:2403.07226*.
7. Logrippo, L. (2025) Data flow security in Role-Based Access Control. *Journal of Information Security and Applications, 90,* 103997.
8. Sandhu, R. S. (1993). Lattice-based access control models. Computer, 26(11), 9-19.
9. Stambouli, A., Logrippo, L. (2019). Data flow analysis from capability lists, with application to RBAC. *Information Processing Letters*, *141*, 30-40.
10. Stambouli, A., Logrippo, L. (2024). Implementation of a Partial-Order Data Security Model for the Internet of Things (IoT) Using Software-Defined Networking (SDN). *Journal of Cybersecurity and Privacy*, *4*(3), 468-493.